KAMU KURUMLARI BİLGİ İŞLEM MERKEZLERİNİN VERİ-SİSTEM GÜVENLİK KALİTESİ BAKIMINDAN DURUM TESPİTİ VE BİR GÜVENLİK KALİTE SİSTEM ÖNERİSİ

Adnan YILMAZ

YÜKSEK LİSANS TEZİ
İSTATİSTİK

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2010
ANKARA

KAMU KURUMLARI BİLGİ İŞLEM MERKEZLERİNİN VERİ-SİSTEM GÜVENLİK KALİTESİ BAKIMINDAN DURUM TESPİTİ VE BİR GÜVENLİK KALİTE SİSTEM ÖNERİSİ

Adnan YILMAZ

YÜKSEK LİSANS TEZİ
İSTATİSTİK

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2010
ANKARA

Adnan YILMAZ tarafından hazırlanan "KAMU KURUMLARI BİLGİ İŞLEM MERKEZLERİNİN VERİ-SİSTEM GÜVENLİK KALİTESİ BAKIMINDAN DURUM TESPİTİ VE BİR GÜVENLİK KALİTE SİSTEM ÖNERİSİ" adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. M. Akif BAKIR
Tez Danışmanı, İstatistik Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile İstatistik Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Prof. Dr. Hamza GAMGAM …….
İstatistik Anabilim Dalı, Gazi Üniversite

Doç. Dr. M. Akif BAKIR …….
İstatistik Anabilim Dalı, Gazi Üniversite

Yard.Doç.Dr. İhsan KARABULUT …….
İstatistik Anabilim Dalı, Ankara Üniversite

Tarih:26/05/2010

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof. Dr. Bilal TOKLU …….
Fen Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Adnan YILMAZ

KAMU KURUMLARI BİLGİ İŞLEM MERKEZLERİNİN VERİ-SİSTEM GÜVENLİK KALİTESİ BAKIMINDAN DURUM TESPİTİ VE BİR GÜVENLİK KALİTE SİSTEM ÖNERİSİ

Yüksek Lisans Tezi

Adnan YILMAZ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Mayıs 2010

ÖZET

Güvenlik ve kalite kavramlarının son zamanlarda ön plana çıkması nedeniyle, Bilgi Güvenliğinin ve Bilgi Güvenliği Yönetiminin kamu kurum ve kuruluşlarındaki mevcut durumlarının, yeniden gözden geçirilmesini acil olarak gündeme getirmiştir. Bu araştırma Türkiye'de kamu kurumlarındaki bilgi işlem birimlerinin bilgi güvenliği konusundaki fiziksel ve politika durumlarını tespit etmek ve bu konudaki mevcut eksiklikleri gidermek için yapılan çalışmaları belirlemeyi amaçlamaktadır.

Bilgi işlem teknolojisindeki donanımsal ve yazılımsal gelişmelerin karşısında Türkiye'deki kamu kurumlarının bilgi güvenliği bakımından durumlarını tespit etmeye yönelik son yıllarda yapılmış bir çalışmanın olmaması, bu çalışmayı yapmayı motive etmiştir. Çalışmanın bulguları kamuda bilgi güvenliği konusunda yapılan çalışmaların yeterli olmadığını, çoğu kurumların belli bir kalite düzeyini yakalayamadığını, genellikle başarı oranı düşük güvenlik yöntemlerinin benimsendiğini ortaya koymuştur. Kurumların mevcut bilgi güvenliği standartlarına uyumlulukları irdelenerek eksik tarafları tespit edilmiştir.

Bu araştırmada e-devlet uygulamaları kapsamında, ihtiyaç duyulan bilgilerin ağ sistemleri üzerinde paylaşıldığı, bilgiye her noktadan erişildiği görülmüştür. Kamu kuruluşlarının bilgi güvenliğini, bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlamak zorunda olmasından dolayı, bu araştırma kurumsal bilgi güvenliğine yönelik mevcut yazılımlar, donanımlar ve insan faktörü noktalarındaki durumu ölçmeye yönelik olarak tasarlanmıştır.

Çalışmada, kurumsal çeşitlilik dikkate alınarak Ankara'da bulunan 82 kamu kurum ve kuruluşuna anket uygulanması yoluyla gerçekleştirilmiştir.

Bilim Kodu **:205.1.013**
Anahtar Kelimeler **:Bilgi güvenliği, Kamu Kurumlarında güvenlik kalitesi**
Sayfa Adedi **:122**
Tez Yöneticisi **:Doç. Dr. M. Akif BAKIR**

A SECURITY QUALITY SYSTEM PROPOSAL AND THE ASCERTAINMENT OF THE FACTS REGARDING DATA –SYSTEM SECURITY QUALITY FOR COMPUTER CENTERS OF PUBLIC BODIES
(M.Sc. Thesis)

Adnan YILMAZ

GAZİ UNIVERSITY
INSTITUTE OF SCIENCE AND TECHNOLOGY
May 2010

ABSTRACT

Due to the fact that, Security and Quality concepts began to stand in the forefront lately, it becomes a necessity to investigate actual status of information security and its administration at public bodies and organizations. This survey aims to determine studies, being carried to ascertain physical and political status of computer centers at governmental institutions.

Reason of which, not being any survey or study at the extend of determining information security in governmental offices in recent years in Turkey, led met o conduct this study. Findings of the study I have carried show that attempts about information security at offices are not enough or effective as well as many governmental bodies do not achieve adequate quality level. Moreover the survey implies that, in general, offices or departments have adapted low success rate solutions regarding information security. At last, compatibility of public bodies with latest information security standards has been examined and any defectiveness has been identified.

In this survey, it is seen that at he context of e-government applications, the information needed are shared via networking systems, being reached at the every access point. Because governmental offices are responsible for

establishing and providing every place, where information is produced, processed or preserved, with information security, this study has been prepared to evaluate current status of software, hardware and human factors at the extend of institutional information security concepts.

During the study, regarding institutional diversity, 82 governmental organizations located in Ankara, have been surveyed.

Science Code :205.1.013
Key Words :Information security, security quality at public bodies.
Page Number :122
Adviser :Assoc.Prof. Dr. M. Akif BAKIR

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla bana çok büyük destekler veren ve yönlendiren Hocam Doç Dr. M. Akif BAKIR'a, bana destek olan hocam Prof. Dr. Hamza GAMGAM'a Anket çalışmasında bana yardımcı olan, Kamu Kurum ve Kuruluşlarda Bilgi İşlem yöneticisi olarak çalışan arkadaşlarıma, hakim Dr. Servet YETİM'e, Sermaye piyasası kurulunda görev yapan Dr. İzzet Gökhan ÖZBİLGİN'e, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli arkadaşım Mehmet Kemal NALÇACI'ya, Nesrin ÇELİK'e teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

Çizelge **Sayfa**

Çizelge **Sayfa**

Çizelge **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AAA	Açık Anahtar Altyapısı
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AR-GE	Araştırma Geliştirme
BCP	Businness Continuity Planing (İş Sürekliliği Planlaması)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BIM	Bilgi İşlem Merkezi
CERT	Acil Müdahale Timi Merkezi
CPU	Merkezi İşlemci Birimi
DISK	Bilgisayar Depolama Birimi
DoS	Denial of Service (Servisi engelleyen saldırı)
DPT	Devlet Planlama Teşkilatı
DTM	Dış Ticaret Müsteşarlığı
EİK	Elektronik İmza Kanunu
E-İMZA	Elektronik İmza
ETKK	Elektronik Ticaret Koordinasyon Kurulu
ITU	Telekominikasyon Birliği
KPSS	Kamu Personel Seçme Sınavı
ÖSS	Öğrenci Seçme Sınavı
PTT	Posta Telefon Telgraf
RAS	Remote Access Services (Uzaktan Erişim Hizmetleri)
SSK	Sosyal Sigortalar Kurumu
TCMB	Türkiye Cumhuriyeti Merkez Bankası
TOBB	Türkiye Odalar Borsalar Birliği

Kısaltmalar	Açıklamalar
TK	Telekominikasyon kurumu
UNICITRAL	Ticaret Hukuk Komisyonu

1. GİRİŞ

Küreselleşme olgusunun gelişiminde önemli etkisi olan bilgi ve iletişim teknolojilerindeki yenilikler, ekonomik ve sosyal yaşamın her alanını ve toplumun tüm kesimlerini çeşitli yönlerden etkisi altına almakta; kamu yönetimi yaklaşımlarını, iş dünyasının iş yapma usullerini ve bireylerin yaşamlarını çok yakından ilgilendirmektedir [Güngören, 2008].

Bilgi ve iletişim teknolojilerindeki gelişmeler, toplumsal dönüşüme neden olarak, "bilgi toplumuna" zemin oluşturmaktadır. Bu bağlamda, bilgi teknolojilerindeki gelişmeler kadar, bilginin üretilmesi, üretilen bilginin yönetilmesi ve güvenliğinin sağlanabilmesi hususları bir problem alanı olarak ön plana çıkmaktadır. Bu değişimlerin kamu yaşamına etkileri Türkiye'nin de bürokratik devletten elektronik devlete geçme yönündeki gelişmelere hem imkân sağlamakta hem de bu gelişmeleri hızlandırmaktadır. Ancak, bilginin çokluğu ve dijital ortamdaki dolaşımı, bilginin yönetimi ve güvenliği konularının önem kazanmasına yol açmıştır.

Bilgi güvenliği dendiğinde, bilginin gizliliği, bütünlüğü, erişebilirliği ve kullanılabilirliği anlaşılmalıdır [Kumaş, 2009]. Bilgi güvenliği politikaları her kuruluş için farklılık gösterse de genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, denetimini, kalitesini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar tüm kamu kurum ve kuruluşlarda genel olarak ifade edilebilmektedir.

Günümüzde internet ve bilgisayar teknolojilerinin kullanımın artması, kurumların iş süreçlerini elektronik ortama taşımaları, "bilgi güvenliği" kavramının çok sık karşımıza çıkmasına neden olmuştur. Böylece, bilgiye sürekli erişimin sağlanması, son kullanıcıya kadar bozulmadan güvenli bir şekilde sunulmasının temini bir zorunluluk haline gelmiştir. Bilgi güvenliğinin sağlanmasında alınacak teknolojik önlemlerin (anti virüs uygulamaları, güvenlik duvarları, saldırı tespit sistemleri,

servis durdurucu işlemlere karşı koruma sistemleri, e-posta filtreleme sistemleri, donanımsal kısıtlamalar vb) yanı sıra, bilgi güvenliği kurumsal süreçlerin bir parçası olarak ele alınmalıdır. Kısaca bilgi güvenliği diskte, iletişim ağında, yedekleme ünitelerinde ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasıdır [Karause, 2007].

Elektronik ortamlarda bulunan bilgilerin her geçen gün katlanarak artmasından dolayı bilgi güvenliğinin ve kaliteli güvenlik ihtiyaçlarının kişisel ve kurumsal olarak en üst seviyelere çıkarılması kaçınılmaz hale gelmiştir. Bunun nedenleri, bilgilerin ağ sistemleri üzerinde paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması ve en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir. Kişi ve kurumların bilgi güvenliğini ve kalitesini sağlamadaki eksikliklerinin yanı sıra, saldırganların saldırı yapabilmeleri için ihtiyaç duydukları yazılımlara internet üzerinden kolaylıkla erişebilmeleri, fazla bilgi birikimine ihtiyaç duyulmaksızın kişisel ve kurumsal bilgi varlıklarına yapılan saldırıları artırmıştır. Bu nedenlerle, bilgisayarları ve ağ güvenlik programlarını yönetmek gittikçe önemli ve zor bir iş haline gelmiştir [Türkiye Bilişim Derneği, 2003]. Bu bağlamda, kurumlar bünyesinde yeni yaklaşımların ve kalite standartlarının uygulanması kaçınılmaz hale gelmiştir. Kamu kurum ve kuruşlarındaki kurumsal bilgi güvenliği, bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve kaliteli insan kaynakları dikkate alınmalıdır [Carlson, ISO17799]. Özellikle devlet yönetiminde bilgi teknolojilerine hızla yönelme, bilginin kalitesi ve bilgi güvenliğine ilişkin hususlarda özel politikalar geliştirme ve bunları uygulamaya sokmada yararlanılacak kılavuzların oluşturulmasını gerektirmektedir. Güvenlik politikası, kurumların güvenlikle ilgili hedeflerin ne olduğunu ve nasıl yönetileceğini de içeren bilgi güvenliği politikası belgesine dayanır [Vural ve Sağıroğlu, 2008]. Bilgi güvenliği politikaları her kuruluş için farklılık gösterse de genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, denetimini kalitesini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar tüm kamu kurum ve kuruluşlarda genel

olarak uygulamaya konulmalıdır [Çetinkaya, 2008].

Bu çalışmada, Türkiye'de kamu kuruluşlarının bilgi güvenliği bakımından bir durum tespiti yapılmıştır. Saha çalışmasıyla çeşitli kamu kurumlarından anketle toplanan bu bilgiler, kamu kurumlarındaki güvenlikle ilgili tespitlere ana kaynaklık oluşturmaktadır. Bu çerçevede imkanlar dahilinde belirlenen 82 adet çeşitli karakteristikteki kamu kurumuna 75 soruluk bir anket uygulanmıştır.

Çalışmanın amacı, bilgi işlem birimlerinin idari yapılaşmasını, bilgi güvenliğinin ve bilgi güvenliği yönetiminin kamu kurum ve kuruluşlarındaki mevcut durumunu, eksikliklerini ve bu bağlamda yapılan çalışmaları ortaya çıkarmaktır. Bu doğrultuda, çalışmanın sonuçları kurumların güvenlik standartlarına uygun olarak belgelenmiş bir bilgi güvenliği yönetim sisteminin bulunup bulunmadığını, güvenlik için gerekli politikaların neler olduğunu, nasıl uygulandığını, uygulamalar sırasında karşılaşılan sorunları ortaya koyarak, kurumlardaki bilgi güvenliğiyle ilgili çalışan sistem ve kurum yöneticilerine kaynak belge olabileceği düşünülmektedir.

2. BİLGİ GÜVENLİĞİ İLE İLGİLİ TEMEL KAVRAMLAR

Bu bölümde bilgi güvenliği ve ilgili temel kavramlar ele alınacaktır.

Bilgi güvenliği, bilginin bir varlık olarak hasarlardan korunmasını ifade eder [Çağlayan, 2003]. Bilgi güvenliği politikası, bilginin aşağıdaki özelliklerinin korunmasını içerir.

a) Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması,
b) Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,
c) Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması [Öztürk, 2008].

Bu çerçevede Bilgi teknolojileri açısından güvenliğin boyutları fiziksel güvenlik, iletişim güvenliği, ve bilgisayar güvenliği olarak sınıflandırılabilir. Güvenlik açığı bunlardan bi,ri veya birkaçında oluşan zayıflıklar veya eksiklikler olarak tanımlanabilir.

2.1. Fiziksel Güvenlik

Fiziksel güvenlik bilginin saklandığı ortamın fiziksel anlamda güvenliği ile ilgili önlemleri kapsar. Bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler fiziksel güvenlikle ilgili önlemlerdir.
Organizasyonlarda çoğu zaman fiziksel güvenlik tek başına yeterli olmamış ve bilgilerin çalınması ve başka kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir [Nazlı, 2010]. Verilerin güvenliğini korumak amacıyla başka tedbirler almak gerekmektedir.

2.2. İletişim Güvenliği

İletişim kavramı veri ve bilginin bir ortamdan diğer bir ortama taşınması olarak tanımlanabilir. İletişim güvenliği bilginin transferi esnasında alınması gerekli önlemler bütününü tanımlar. İletişim sırasındaki bilginin hedefe ulaşmadan önce başka kişiler tarafından ele geçirilmesi ve içeriğinin öğrenilmesi riski her zaman mevcuttur. Şifreli mesajlar özellikle askeri iletişimlerde kullanılmaktadır. Bilgi işlem ve iletişim ile ilgili sistem açma/kapama, yedekleme, cihazların bakımı, bilgisayar odasının kullanılması, gibi sistem faaliyetleri prosedürlere bağlanmış olmalı ve kontrol altında tutulmalıdır [Nazlı, 2009].

2.3. Bilgisayar Güvenliği

Kurum ve kuruluşlar birçok veri ve bilgiyi elektronik ortamda tutmaya başlamıştır. Dolayısıyla, güvenlik kavramını bütünleyen önemli bileşenlerden birisi de bilgisayar güvenliğidir. Bilgisayar güvenliği problemi bilgisayara saldırı biçiminde gerçekleşip, kısaca bir kişinin bilgisayarına ondan izin almaksızın girmek ve bir takım işlemler (okuma, kayıt, silme gibi.) yapmayı tanımlar. Buna bilgisayar terminolojisinde, makineyi "hack" etmek te denilmektedir. Dünyanın herhangi bir yerindeki internete bağlı bir bilgisayardan giriş yapılma ihtimali vardır. Bu giriş işlemleri için oldukça değişik yollar kullanılabilmektedir. Bilgisayar güvenliğini tehdit eden problemler, bizzat kişinin, başkasına ait bir bilgisayarı habersiz bir şekilde başına geçip kullanması, bilgisayara e-mail, chat programları, disket veya ağdan yararlanarak trojen adı verilen ve bilgisayara dışarıdan girilmesini kolaylaştıran programların yüklenmesi, ağda verilen paylaşımlardan yararlanarak bilgisayara giriş, güvenirliği bilinmeyen web sayfalarında dolaşmak biçiminde gerçekleşmektedir [http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik].

2.4. Saldırı Türleri ve Kurumlarda Görülen Açıklar

Saldırılar bilimsel araştırmalarda detaylı olarak irdelenmekte ve oluşturdukları tehditlere karşı güvenlik önlemleri geliştirilmeye çalışılmaktadır. Ancak bu saldırılara her gün yeni türler eklenmekte, aynı hızla da çözümler üretilmeye çalışılmaktadır. Genel olarak güvenlik açıkları hatalı programlama, hatalı yapılandırma ve güncelleme yapılmamasından kaynaklanmaktadır [http: //www.izafet.com/güvenlik-ve–güvenlik-aciklar].

2.5. BİM'lerin Zayıf Noktalarına Yönelik Tehdit Biçimleri

Bugüne kadar yaşanan tecrübelerden hareketle, bilgi işlem merkezi sistemlerinin karşılaştığı tehditler kısaca aşağıdaki gibi özetlenebilir.

Tarama (Scanning): Sisteme değişken bilgiler göndererek sisteme giriş için uygun isim ve parolaları bulmak için kullanılır.
Sırtlama (Piggybacking): Yetkili kullanıcı boşluklarından ve hatalarından yararlanıp, aynı yolu kullanarak sisteme girme.
Dinleme (Eavesdropping): İletişim hatlarına saplama yapmak.
Casusluk (Spying): Önemli bilginin çalınmasına yönelik aktiviteler.
Yerine geçme (Masquerading): Yetkisiz bir kullanıcının yetkili kullanıcı haklarını kullanarak sisteme girmek istemesi.
Çöpleme (Scavenging): Gerçekleştirilen işlem sonucu kalan kullanılabilir bilgilerin toplanması.
Arkaya takılma (Tailgating): Dial-up bağlantı düşmelerinden veya işlemin tamamlanmasından sonra hattı elinde bulundurarak sisteme girme
Süperzap yöntemi (Superzapping): Sistem programının gücünden yararlanarak işlem yapma.
Truva atı (Trojan Horse): Dışarıdan cazibesine kapılarak indirilen veya sisteme kopyalanan programlardır.
Virüsler :Kendi başına çalışamayan, ancak başka programlar aracılığı ile çalışıp

kendini taşıyan programlardır.

Solucanlar (worms): Kendi kendini çalıştırabilen ve kopyalayabilen bir programdır.

Kapanlar (Trap doors): Tasarımcıların ve geliştiricilerin sistem bakımından yararlanmak üzere bıraktıkları programlardır. Kötü amaçla kullanılabilirler.

Mantık Bombaları (Logic bomb): Önceden belirlenmiş koşullar gerçekleşince harekete geçen programlardır.

Salami teknikleri (Salami Techniques): Dikkati çekmeyecek büyüklükte sistem kaynağı veya kaynakların zimmete geçirilmesi.

Koklama (Sniffing): Ağ üzerindeki paketlerin izlenmesi.

Aldatma (Spoofing): Ağa saplama yapılarak bilgilerin değiştirilmesi adres değişikliği yapılması.

Kırmak (Cracking): Sistem güvenlik önlemlerinin kırılması

Bilgi işlem sistemlerine yönelik bu tehditler, bunlarla sınırlı kalmayıp, zaman içinde doğal olarak yeni tehdit türleri eklenecektir. Yaygın saldırı türleri aşağıdaki şekilde sıralanmıştır.

2.6. Yaygın Saldırı Türleri

Günümüzde bilgisayar sistemlerinin güvenliği artırılmasına rağmen, bu sistemlere yapılan saldırılar da artmaktadır. Bu sistemlerin sahip olduğu güvenlik yapısını aşmaya çalışan saldırılar ile alınan karşı tedbirlerin sayısının da arttığı ve farklılıklar gösterdiği gözlenmiştir [Canbek ve Sağıroğlu, 2007].

Saldırganlar ya da "Hacker"lar saldırı amacıyla değişik araçlar kullanırlar. Saldırganlar, öncelikle saldırılacak hedefin IP adresini ve geçilen yönlendiricileri tespit ederler. Goffer, portscan, finger gibi yazılımları kullanarak ilk erişimde sistem hakkında daha detaylı bilgi toplarlar. Daha sonra bu topladıkları detaylardan elde ettikleri bilgileri sistemlerin açıklarını tespit etmek için kullanırlar. Çeşitli kullanıcı yetkilerini arttırabilirler, kullanıcıların bilgisayarda yaptığı faaliyetlerin loglarını silerek, izlerini yok ederler. Sistemden çıkarken arka kapı, Truva atı bırakarak

sisteme ilerideki ulaşımını daha kolay hale getirirler. Hackerlar saldırı programını kendileri hazırlayabildiği gibi, bu programlar hackleme ile ilgili web sitelerinden de temin edilebilmektedir.

Bu yöntemler sonucunda bazı zararlı program parçaları bilgisayarlara yerleştirilerek sistemlere çeşitli zararlar verilebilir. Nereden gelirse gelsin saldırı türleri birbirlerine benzerlik göstermektedir. Bu nedenle yaygın saldırı türleri aşağıda belirtilmiştir.

2.6.1. Virüsler

Genelde normal bir programa eklenmiş küçük kod parçacığıdır. Kendisini yeniden üretebilir (iletişim ağında kolayca yayılabilir), kendisini başka programlara (örneğin java script) ekleyebilir. Bazı yok edici, yıkıcı etkileri olabilir. Etkisini hayata geçirebilmesi için virüs içeren programın çalıştırılması gerekir. Bazı virüsler hacker gibi davranarak çalıştığı bilgisayarların yönetici haklarını ele geçirebilir.

2.6.2. Kurtcuklar

Virüslere benzerler. Virüslerden farklı olarak, bilgisayar ağlarında bağımsız bir şekilde dolaşıp, yayılabilirler. Genelde disk üzerinde değil hafızada bulunurlar.

2.6.3. Truva atları

Genelde gerekli bir program gibi gözüken ama arka planda yok edici etkisi olan programlardır (örneğin, virüslerden kurtulmanızı sağlayacağını iddia eden ama aslında bilgisayarınıza virüs yerleştiren programlar). Bazı Truva atları da arka kapı açarak sisteme kolay erişim sağlarlar.

2.6.4. Arka kapılar

Truva atları ile karıştırılabilir olmasına rağmen farklı özellikleri vardır. Bir arka kapı, yetkili kullanıcıya yazılımı değiştirme imkanı verir. Oyunlarda sıkça kullanılan daha çok kaynak ve üst seviyelere geçmeye yarayan ve *cheat codes* denilen hilelere benzerler. Fakat bu bağlantı onayı (connection authentication) veya elektronik ileti benzeri uygulamalar için de geçerlidir. Çünkü bu uygulamalar da üreticisinin belirlediği gizli bir geçişe imkan verebilir.

2.6.5. Servisi engelleyen saldırılar (Denial of Service: DoS)

Bu saldırı türünde sistemdeki programlara virüs bulaşmamaktadır. Ancak, sistem kapasitesinin üstünde yüklenerek kullanılamaz hale getirilir. Örneğin, 10 dakika içinde 100.000 e-posta gelmesi durumunda e-posta hizmeti veren sunucular işlevlerini göremez hale gelebilmekte ve sistem yaygın tabiriyle "çökebilmektedir". Adından anlaşılacağı üzere, burada açıklanan yöntem normal çalışmayı engelleyen, durduran bir saldırı türüdür.

2.6.6. Mantıksal bombalar

Mantıksal bombalar çeşitli etkilere sahip, kasıtlı olarak zarar veren program parçalarıdır. Sistem kaynaklarına (bellek, hard disk, CPU, vb.) büyük zararlar verebilir, dosyaların mümkün olduğunca hızlı yıkımını sağlayabilirler. Bu saldırı türü, kullanıcıların dosyaların içeriğini yeniden oluşturmalarını önleyerek dosyaları tekrar yazar ve olabildiğince uzun bir zaman saklı kalarak dosyaları el altından yıkabilir. Genellikle, basit ulaşım haklarının uygulandığı düşünülürse, mantıksal bombalar şifre dosyalarının bir internet adresine gönderilmesi yoluyla sistem güvenliğini tehdit ederler.

2.6.7. Mesajlaşma yazılımları

Peer to peer (eşdüzey) trafik olarak da adlandırılan, yahoo messanger, msn messanger, kaza, icq gibi bu yazılımlar kullanıldığında arada hiç aracı olmadan sanki karşılıklı telefon görüşmesi yapıyormuş gibi haberleşme ve dosya transferi için kullanılmaktadır. Bu tür iletişim yoluyla yapılan dosya transferlerinde bazı kontroller yapılamadığından (anti-virüs, içerik kontrolü gibi) kullanıldıkları sistemleri saldırıya açık hale getirebilmektedirler.

2.6.8. Phishing

Kısaca bir internet sitesinin benzer bir web ismi de kullanarak taklit edilmesidir. Kişilerin gizli şifre ve mali bilgilerinin (kredi kartı numaraları vb.) elde edilmesi için sahtekarlarca hazırlanan bir tuzak ve aldatma yoludur. Elektronik ticaret veya bankacılık uygulamaları için sahte giriş ekranları oluşturularak ziyaretçilerin yanıltılması ve sonucunda kullanıcıya ait önemli bilgilerin ele geçirilmesi mümkün olabilir. Örneğin bu tip saldırılara karşı bankalar e-posta yoluyla kullanıcı adı ve şifre istemezler.

2.6.9. E-postalar

E-postalar genellikle yukarıda sözü geçen zararlı yazılımların iletilmesinde ve bilgisayarlara yerleştirilmesinde en yaygın olarak kullanılan araçlardır. Bilinmeyen yerlerden gelenlerin açılması risk oluşturduğundan kesinlikle açılmamalıdır ve özellikle kişilerden bir şeyler yapması istenen e-postalara itibar edilmemelidir. Bilinmeyen web linklerine ve mesaj/uyarı butonlarına basılmamalıdır.

3. BİLGİ GÜVENLİĞİNİN ÖNEMİ VE BOYUTLARI

Güvenlik konusundaki genel yanılgı tehdidin sadece bilgisayar virüsleri veya sistemin yedeklenmesine yönelik çabalardan ibaret olduğu yaklaşımıdır. Bu düşünce doğal olarak beraberinde güvenlik duvarları ve yedekleme yöntemlerinin uygulanma zorunluluğunu getirmektedir. Bunun sonucu olarak da güvenlik ile ilgili ortam sistem ile sınırlı kalmaktadır. Bilgisayar sistemleri güvenliği, doğru ve etkili bir şekilde sağlamak korumak için alınacak tedbirlerde, güvenliği sürekli ve önlemleri canlı tutan olarak ifade edilebilecek güvenlik yaşam döngüsü mutlaka uygulanmalı ve bu çerçevede karşılaşılacak zayıflıklar ve eksiklikler giderilmelidir [Canbek ve Sağıroğlu, 2007].

Bilgi teknolojilerindeki hızlı gelişme, bilginin işlenmesi ve iletilmesindeki yeni kolaylıklar bilişim sistemlerinin sınırlarını oldukça genişletmiştir. Bilginin istenen yer ve zamanda sunulması ve bilginin kaynağından toplanması bilgiyi sistemin her noktasına taşımıştır. Bu durum doğal olarak güvenlik sınırlarını da genişleterek, bilginin yönetimini zorlaştırmış ve riskleri artırmıştır. O nedenle, yeni tehdit unsurları sadece sistemleri etkisiz bırakmakla kalmayıp, kişisel, ticari ve ulusal saygınlığı ve geleceği ile genel etik kuralları da etkiler hale gelmiştir. Önemli kamu bilgilerinin yetkisiz ellere geçmesi, kamu hizmetlerinin aksatılması, sistemlere zarar verilmesi, bilgilerin değiştirilmesi, önemli araştırma bilgilerinin elde edilmesi yani ulusal bilgi güvenliği, vatandaşlara ilişkin bilgilerin amacı dışında kullanılması kişisel bilgilerin mahremiyeti, ticari bilgilerin elde edilmesi ve güvensizlik ortamlarının yaratılması, elektronik ticaret ve sayısal imza gereksinimleri, güvenliğin önemi ve boyutunu açık alarak ortaya koymaktadır.

Bir bilgi sisteminin ise, fiziksel ortam, sistemler (bilgisayarlar), yan donanımlar, iletişim ortamları, iç ve dış bağlantılar (ağlar), depolama birimleri, yazılımlar ve kullanıcılardan oluştuğu düşünüldüğünde sorunun teknik boyutu da ortaya çıkmaktadır.

Bilgi sistemleri güvenliğine yönelik önlemlerin başarısı tehdit ve yapılan hatalardan kaynaklanan zâfiyetlerin bilinmesine bağlı olarak etkilenecektir. Bu nedenle, tehditler ve zayıflıkların neler olabileceğini ve nerelerden kaynaklandığının bilinmesi gerekir.

3.1. Bilgi İşlem Merkezlerinin Zayıf Noktaları

Bilgi işlem merkezlerinin incelenmesine yönelik yapılan çalışmalar aşağıda sıralanan zayıf noktaları tespit etmiştir.

- Sistem odalarının giriş ve çıkış denetimlerinin olmaması,
- Yangın, sel, nem ve rutubet gibi çevresel faktör etkileri,
- Manyetik ortamların kolay erişilebilir açık yerlerde bırakılması,
- Donanım ve yazılımlardan kaynaklanan zayıflıklar,
- İletişim hatlarının uygun ve ağ altyapısının standartlara uygun olmamasından kaynaklanan zafiyetler,
- Elektromanyetik yayılmanın kontrol edilmemesi,
- Kullanıcı dikkatsizlikleri ve hatalarından kaynaklanan zafiyetler,
- Terminallerin kapatılmadan ve parola korumasız bırakılması,
- Görevden ayrılan kullanıcıların erişim haklarının kapatılmaması,
- Güvenlik loglarının izlenmemesi,
- Sistemi izlemede yetersizlikler ve gözden kaçmalar,
- Raporlama prosedürünün ihlal anında yeterince işletilememesi,
- Arızalı disklerin içindeki bilgilerle servise gönderilmesi,
- Yedekleme sıklığının ayarlanamaması,
- Çalışma odalarına misafir kabul edilmesi,
- Parolaların kolay hatırlanabilecek şekilde verilmesi,
- Parolaların değiştirilme frekansının uzun tutulması,
- Bilinçli kullanıcılardan kaynaklanan zafiyetler
- Kullanıcıların bilgileri kendi çıkarlarına uygun kullanmaları,

- Bu tür zayıflıklar ve güvenliği tehlikeye sokacak tehlikeli davranışlara benzer daha çok sayıda örnekle genişletmek mümkündür [Bilişim sistemleri güvenliği el kitabı, 2006].

3.2. Bilgi İşlem Merkezlerindeki Tehditler

Bugüne kadar yaşanan tecrübelerden hareketle, bilgi işlem merkezi sistemlerinin karşılaştığı tehditler kısaca aşağıdaki gibi özetlenebilir.

*Tarama (Scanning):*Sisteme değişken bilgiler göndererek sisteme giriş için uygun isim ve parolaları bulmak için kullanılır.

*Sırtlama (Piggybacking):*Yetkili kullanıcı boşluklarından ve hatalarından yararlanıp, aynı yolu kullanarak sisteme girme.

*Dinleme (Eavesdropping):*İletişim hatlarına saplama yapmak.

*Casusluk (Spying):*Önemli bilginin çalınmasına yönelik aktiviteler.

Yerine geçme (Masquerading): Yetkisiz bir kullanıcının yetkili kullanıcı haklarını kullanarak sisteme girmek istemesi.

*Çöpleme (Scavenging):*Gerçekleştirilen işlem sonucu kalan kullanılabilir bilgilerin toplanması.

*Arkaya takılma (Tailgating):*Dial-up bağlantı düşmelerinden veya işlemin tamamlanmasından sonra hattı elinde bulundurarak sisteme girme

*Süperzap yöntemi (Superzapping):*Sistem programının gücünden yararlanarak işlem yapma.

*Truva atı (Trojan Horse):*Dışarıdan cazibesine kapılarak indirilen veya sisteme kopyalanan programlardır.

*Virüsler :*Kendi başına çalışamayan, ancak başka programlar aracılığı ile çalışıp kendini taşıyan programlardır.

*Solucanlar (worms):*Kendi kendini çalıştırabilen ve kopyalayabilen bir programdır.

*Kapanlar (Trap doors):*Tasarımcıların ve geliştiricilerin sistem bakımından yararlanmak üzere bıraktıkları programlardır. Kötü amaçla kullanılabilirler.

*Mantık Bombaları (Logic bomb):*Önceden belirlenmiş koşullar gerçekleşince harekete geçen programlardır.

*Salami teknikleri (Salami Techniques):*Dikkati çekmeyecek büyüklükte sistem kaynağı veya kaynakların zimmete geçirilmesi.

*Koklama (Sniffing):*Ağ üzerindeki paketlerin izlenmesi.

*Aldatma (Spoofing):*Ağa saplama yapılarak bilgilerin değiştirilmesi adres değişikliği yapılması.

*Kırmak (Cracking):*Sistem güvenlik önlemlerinin kırılması

Bilgi işlem sistemlerine yönelik bu tehditler, bunlarla sınırlı kalmayıp, zaman içinde doğal olarak yeni tehdit türleri eklenecektir.

4. KAMUDA BİLGİ YÖNETİMİ VE BİLGİ GÜVENLİK POLİTİKALARI

Bilgi yönetimi, verilerin toplanması, düzenlenmesi, kayıt altına alınıp bilginin üretilmesi, paylaşılması, kullanılması ve değerlendirilmesine ilişkin tüm süreçlerin yönetimidir. Bilgi yönetiminin temel konusu bilgi ve bilgiye ait işlemlerdir. Bu işlemlerin hedefi bilginin en verimli biçimde kullanımının sağlanmasıdır. Bunun için de bilgi yönetiminin ana hedefi doğru bilginin, doğru kişilere, doğru zamanda iletimini sağlamaktır.

Bilgi yönetiminin kendisi yeni bir kavram olmasına rağmen , kurum ve kuruluşlar her zaman bilgi yönetimi uygulamalarını kararlar almak veya hizmetler üretmek için kullanmışlardır. Hiçbir kurum ve kuruluş bilgiyi elde etmeden ve çalışanlarına aktarmadan ayakta kalamaz . Bilgi özellikle üretimde bir zenginlik oluşturma kaynağıdır. Yeni bilişim ve iletişim teknolojileri nedeniyle hızla değişen koşullara adapte olmak için bilgi çok önemli bir araç olarak kullanılabilir [Akçal, T.C. Kültür ve Turizm Bakanlığı].

Bilgi yönetiminin başarısı açısından kurumlarda işbirliği, bilgi ve fikir paylaşımının oluşturulabilmesi büyük bir önem taşımaktadır. Diğer bir deyişle, sadece teknolojik araçların kullanımı ile kaliteyi yakalamak ve başarıya ulaşmak mümkün değildir.

Bir kurumun bilgi yönetimi sürekli yaşayan bir uygulamadır. Kurumun kendi gereksinimleri doğrultusunda özel olarak geliştirilmelidir. Bu kapsamda her kurumun bilgi yönetim sistemi diğerinden farklılık gösterse de genel olarak bilgi yönetiminin kurulması için şu aşamalar gerçekleştirilmelidir.

- Analiz
- Bilgi yönetimi ve kurumsal iş hedeflerinin ilişkilendirilmesi
- Altyapı tasarımı
- Bilgi toplama süreci
- Bilgiyi kullanılabilir bilgiye dönüştürme süreci

- Bilgi yönetimi sisteminin tasarlanması
- Bilgi yönetimi sisteminin geliştirilmesi
- Bilgiyi örgütsel uygulamalarda kullanma süreci
- Bilgi yönetimi sisteminin değerlendirilmesi, ihtiyaç varsa yeniden düzenlemelerin yapılması ve bilgiyi koruma süreci.

Bilgi yönetimi süreçleri birbirleriyle bağımlı ve iç içe geçmiş süreçlerdir. Bu nedenle, bilgi bir bütünlük içersinde ve koordineli bir biçimde yönetilmeleri gerekir. Bu aşamalar, uzman personelden oluşmuş komisyonlarca gerçekleştirilmelidir. Örgütsel yapıda elde edilen veya yaratılan bilginin kullanılmasında çalışanları teşfik edecek şekilde tasarlanmalı ve yüksek düzeyde bilgi paylaşımını da sağlamalıdır. [Demircan, Yıldız ve Dur, 2010]. Böylece, mükerrer bilgi, bilgi kaybı gibi sorunların önüne geçilmektedir. Kamu yöneticilerinin büyük bir kesimi hizmetlerin geliştirilmesi ve performans hedefleri konusunda düşük bir duyarlılığa sahiptirler. Kendilerine çok genel hedefler seçerler ve kamu yararını her şeyin üstünde gördüklerini söylerler. Bu nedenle kamu kurumlarındaki geleneksel iletişim kültürü bilgi yönetiminin en büyük engeli olarak ortaya çıkmaktadır. Gelişen teknolojik olanakları kullanmanın yanı sıra, kurumlar öncelikleri doğrultusunda bilgi yönetiminin amaç ve politikalarını açık biçimde belirlemeli ve tanımlamalıdır. Son yıllarda verimlilik geliştirme çalışmalarında özellikle performans yönetimi, yetki alanı, yetki devri, kalite yönetimi ve enformasyon teknolojisi gibi konular ön plana çıkmaktadır [Özgüler C., 2005]. Bunun yanı sıra, kurum çalışanlarının gönüllü katılımının ve bağlılığının sağlanması, Etkin bir bilgi yönetimi, Kamu kurum ve kuruluşlarında verimlilik ve kalite hedeflerine ulaşma yolunda kesin başarıyı getirecektir.

4.1. Kurumlarda Bilgi Güvenliği

Kurumsal bilgi güvenliği, kurumsal iş süreçlerine uygun olarak yapılacak, TSE ISO 27001 “Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri” standardına uygunluk çalışmaları kapsamında ele alınmalıdır. Bu kapsamda amaç; kaliteli bir ortamda

gizliliğin, bütünlüğün ve kullanılabilirliğin sağlanması olmalıdır [TSE ISO 27001, 2006].

Bilgi güvenliği kurumsal süreçlerin bir parçası olmalıdır. Bu amaçla, kurumlar kendi iş süreçlerine uygun bir güvenlik politikası oluşturmalı, bunu yazılı hale getirerek tüm personeline duyurmalı, bu politikanın kurum kültürü haline gelebilmesi için de gerekli eğitimleri sağlamalıdır.

Bilgi envanteri'nin çıkartılması ve sınıflandırılması, saklanması, uygulama güvenliği, fiziksel güvenlik, iş sürekliliği, bilgi hakkı yönetimi ve şifreleme, personel eğitimi, üçüncü şahıslar ile çalışma prensipleri, bilgi güvenliği politikasının ana unsurlarıdır. Temel prensiplerin belirlenmesi ve uygulamalarının takibi gibi konular Bilgi İşlem Merkezlerinin öncülüğünde ilgili birim temsilcilerinin oluşturduğu ve üst yönetimin doğrudan desteği altında çalışan komisyonlarca yapılmalıdır.

4.2. Bilgi İşlem Merkezlerinin Güvenliği

Bilgi işlem merkezleri kuruluşundan itibaren, bilgi sisteminin işletmesinden, bakım ve onarımından, sorumlu oldukları tüm bilişim teknolojilerinden, kaynakların işletilmesine kadar tüm ilgili usul ve esasları belirlemeli ve tanımlamalıdır.

Bilişim teknolojileri kaynaklarının her birisi için tanımlanacak sorumlu yöneticinin/yöneticiler için, bu kaynaklar ve üzerindeki verilerin bütünlüğü, güvenliği ile ilgili sorumluluklarının tanımlanmasının yanı sıra, kaynakların kuruluşuna ve işletilmesine ilişkin belgelerin hazırlanması ve saklanması ile ilgili sorumluluklarının tanımlanması gereklidir. Sistem güvenliğine yönelik olarak, her bir kaynağın yedeklenmesi, geri yüklenmesi, kaynağın çökmesi durumunda uygulanacak işlemleri içeren adımların tanımlanması zorunludur.

4.3. Kamuda Bilgi Güvenlik Politikalarının Oluşturulması

Hazırlanacak Bilgi Güvenlik Politikası, bilgi güvenliğinin sağlanması için kurum çapında kullanılacak bilgi güvenliğinin omurgasını oluşturur. Yapının sağlıklı ve kaliteli olabilmesi için bu politika ile birlikte kullanılacak ilişkili alt politikaların ve prosedürlerin de hazırlanması gerekmektedir. Bilgi Güvenlik Politikaları kurum yönetimi tarafından onaylandıktan sonra iki aşama olarak bilgi güvenliği yapısının oluşturulması ve Bilgi Güvenlik Politikası'nın uygulanması hedeflenmelidir.
Bu politika ile Kurumda bilgi güvenliğinin sağlanabilmesi için kurum stratejisinin belgelenerek, kontrol edilebilen, etkili güvenlik önlemlerinin alınması gerekmektedir.

4.4. Bilgi Güvenlik Politikalarının Kapsamı

Kurumda bilgi güvenliğinin sağlanabilmesi için personel, fiziksel ve çevresel güvenlik, iletişim ve operasyon yönetimi, erişim kontrolleri, sistem geliştirme ve bakımı vb. konularda uygulanacak standartların, kontrollerin ve kuralların belirlenmesi hedeflenmelidir. Dolayısıyla, Bilgi Güvenlik Politikası, tüm bilişim sistemlerini ve kurumun tüm kaynaklarını kapsamalıdır. Politika geliştirmede, kurum gereksinimleri ve riskler göz önüne alınarak,

- Bilgi Güvenlik politikası, alt politika ve prosedürlerinin hazırlanması, onaylanması.
- Bilgi Güvenlik politikası nın kurumda duyurulması.
- Bilgi Güvenlik organizasyonu nun oluşturulması.
- Durum tespitinin yapılması
- Bilişim sistemlerinde önemli varlıkların tespit edilmesi
- Risk analizi ve risk yönetimi yapısının oluşturulması
- Tespit edilen acil aktivitelerin hayata geçirilmesi
- Bilgi güvenlik planlarının ve iş devamlılık planlarının hazırlanması

- Politikaların ve prosedürlerin uygulandığının denetlenmesi ve güncellenmesi çalışmalarının tamamlanması hedeflenmelidir.

4.5. Kamuda İş Dağılım Yapısı

Bilgi Güvenlik Politikalarını oluştururken ekip çalışması ve iş bölümlerinin yapılması gerekmektedir. Bu ekipler Bilgi Güvenlik Birimi, Bilgi İşlem Birimi ve kurumun diğer birimleri olarak sıralanabilir. Kamu kurumlarında bilgi güvenliği biriminin görevleri aşağıdaki faaliyetleri kapsamalıdır.

- Proje koordinasyonu sağlanması,
- Proje raporlama ve dokümantasyonun sağlanması,
- Kapsam ve detay çalışmaları için kullanılacak standartların ve uygulanacak yöntemin yer aldığı, yol gösterici dokümanların hazırlanması;
- Bilgi güvenlik politikasının kapsam ve içeriğinin belirlenerek hazırlanması;
- Bilgi güvenlik politikasının alt politikaları ve prosedürlerinin belirlenerek hazırlanması;
- Birimlerden gelen isteklerin değerlendirilerek gerekli görülmesi durumunda proje dokümanlarına yansıtılması;
- Proje çalışmalarının planlanması, varlıkların belirlenmesi, sınıflandırılması, risk analizi, bilgi güvenlik planları, iş devamlılık planları hazırlanması gibi proje aktiviteleri için kullanılacak yöntem, standartların, kalitenin ve yardımcı dokümanların hazırlanması;
- Yapılacak çalışmalar için eğitimlerin verilmesi;
- Birimlerden gelen çalışma sonuçlarının değerlendirilmesi, incelenmesi, takibi ve kontrolünün sağlanması gereklidir.

5. KAMU KURUM VE KURULUŞLARINDA İŞ SÜREKLİLİĞİ

İş sürekliliği planlaması, bir kurumun çalışmalarının devamlılığını sağlamak amacıyla bilişim altyapısının kesintisiz veya olağanüstü durumlarda en az kesintiyle hizmet vermesi için yapılması gerekenleri içerir.
Bilişim tabanlı servislerin kesintiye uğraması/aksamasını gerektirecek durumlar şunlardır:

- Donanım arızaları
- İletişim hatları veya elektrik kesintileri
- Kötü niyetli yazılımlar (virüs, solucan) ve internet tabanlı saldırılar (hacking)
- Doğal felaketler (deprem, volkanik patlama)
- Yangın, su basması
- Terör olayları

Yukarıdaki durumların herhangi birinin gerçekleşmesi durumunda iş sürekliliğin sağlanması için önceden yapılması gereken çalışmalar ve alınması gereken önlemler ise aşağıdaki gibi sıralanabilir.

- Servis kesintisine yol açabilecek tüm durumlar için ilk olarak yapılması gereken düzenli bir biçimde sistemdeki tüm kritik yazılım ve sunucuların yedeklenmesidir. Hangi sistemlerin, ne ölçüde, kimin tarafından, hangi sıklıkla, nereye ve hangi yöntemle yedeğinin alınacağı belirlenmeli, yedekleme işlemi buna göre yapılmalı ve alınan yedeklerin çalışabilirliği düzenli olarak kontrol edilmeli.
- Donanım arızalarına karşın kritik sistemlerin donanım olarak yedekleri (redundancy) tutulmalı.
- Elektrik kesintileri için UPS ve jeneratör sistemleri kurulmalı.

- İnternet çıkışı ve diğer kritik iletişim hatlarının sürekliliği için alternatif çözümler bulunmalı. (İki ISP'den servis almak, özel devrelerin yanında VPN kullanmak)
- Bilgi sistemleri altyapısının güvenliğinin sağlanması bu sistemlerin kesintisiz çalışması için çok önemli olduğundan güvenli bir bilişim alt yapısı oluşturulmalı.
- Herhangi bir felaket sonucunda kullanılan binanın hasar görmesi durumunda kesinti yaşanmaması için ikincil çalışma ortamlarının hazır tutulmalı.

Yaşanması muhtemel felaket durumlarına karşın Felaket Kurtarma Planlaması (Disaster Recovery Planning) yapılmalı ve acil bir durumda yapılacak işler (acil durum prosedürü) ve sorumlular (acil durum masası) önceden belirlenmelidir. Son olarak iş sürekliliği kapsamında alınan tüm önlemler ve planlanan çalışmalar tatbikatlar ile denenmelidir. Kurum veya kuruluşta iş sürekliliğin sağlanması için yöneticilerin eğitimi ve bilinçlendirilmesi, ağ güvenliğini zedeleyen hataların ortadan kaldırılması ve bilinçlendirmenin öneminin benimsetilmesi gerekmektedir.

5.1. Kamu Kurum Ve Kuruluşlarda Kullanıcı Ve Yöneticilerin Eğitimi Ve Bilinçlendirilmesi

Eğitimin amacı çalışanları bilişim güvenliği konusunda bilinçlendirmek ve insan hatasından doğabilecek riskleri en aza indirmektir. Burada eğitilmesi gerekenler hem çalışanlar hem de yöneticilerdir.

5.2. Bilgisayar Ağ Güvenliğini Zedeleyen Başlıca Yönetim Hataları

Bilgi güvenliğini etkileyen başlıca yönetim hatalarının başında güvenlik ağı için eğitimsiz kişilerin atanması ve bu kişilere ne gerekli eğitimin, ne de işlerini doğru düzgün yapabilmek için gerekli zamanın verilmemesi gelmektedir. Bunun sonucu olarak yöneticilere doğru bilgi akışı sağlanamamaktadır.

Bilgi teknolojilerinde eğitim almamış bir yöneticinin fiziksel güvenlikten anladığı basit tedbirler olabilir, fakat etkin bir bilgi güvenliğinin ne olması gerektiği ve nelere yol açabileceğini takdir edebilmesi kolay olmayabilir.

Güvenlik, kurumlarda bir defalık kurulacak bir sistem olarak algılanmakta ve güvenliğin operasyonel yanları ile uğraşılmamaktadır. Oysa, saldırıların türleri ve araçları teknoloji ile birlikte sürekli olarak değişmektedir. Temel olarak sadece bir güvenlik duvarının yeterli olduğu kanısı hakimdir.

Yöneticiler eldeki bilgilerin ve organizasyonel saygınlığın değerini takdir edememekte, kimlerin hangi nedenlerle bu bilgilere saldırabileceğini değerlendirmekte eksik kalmaktadırlar. Kurumdaki bilgilerin envanteri'nin çıkarılması ve bunların bilgi güvenliği açısından sınıflandırılması çok önemlidir.

Yöneticilerde ve kurumlarda sorunlara reaksiyon göstermeye yönelik, kısa vadeli çözümler uygulamaya konmakta ve bu nedenle sorunların kısa süre içinde tekrarlanması engellenememektedir.

Yöneticilerin kendileri bilgi teknolojilerine olan uzaklıklarından dolayı güvenlik önlemlerine yeteri kadar önem vermeyebilmektedirler. Örneğin kullanıcı adı ve şifresini çalışanına veren, dolayısıyla yetkilerini onlara kullandıran yöneticilerin sayısı az değildir. Bu durum ıslak imza yerini alan elektronik imza için bile değişmemektedir.

5.3. Kamuda Bilinçlenmenin Önemi ve Alınması Gereken Önlemler

Bilgi güvenliği bağlamındaki sorunlara getirilecek çözümlerden birisi kullanıcının esnekliğini en aza indirmektir. Örneğin iris tanıma yoluyla bilgisayara girip onay vermek zorunda olan bir yönetici yetkilerini kendisi kullanmak ve bilgi teknolojileri bilgisini artırmak zorundadır [Akman, 2004].

Mobil bilgisayarlar, sipariş üzerine yazılan uygulama yazılımları, kuruma uzaktan erişim (RAS), internet gibi konular güvenliği tehdit eden unsurlardır. Bilişim sistemlerinin altyapısında caydırıcı, etkin güvenlik önlemleri alınmalıdır. Şifre kullanımı, kriptolama, güvenlik duvarı, yedekleme politikaları çok net olarak tanımlanmalıdır.

Atılması gereken diğer bir adım da çalışanların güvenlik konusunda bilinçlendirilmesi ve güvenlik sorununun tüm çalışanlar arasında paylaştırılarak, sorumluluğun dağıtılmasıdır. Her çalışan konunun önemini anlayarak sahip çıkmalıdır.

Kurum içinde uygulanan güvenlik politikaları yazılarak çalışanlara dağıtılmalı ve alınan önlemlerin nedenleri herkese anlatılmalıdır. Güvenlik politikaları, bir güvenlik sorunu ile karşı karşıya kalındığında, kurum içinde nasıl davranılması gerektiğini, kimlerin hangi noktalardan sorumlu olduğunu da açıkça belirtmelidir.

Yönetim kademesinde çalışanlara büyük görevler düşmektedir. Yöneticilerin vizyon sahibi olmaları nedeni ile oluşabilecek sorunları önceden tahmin ederek proaktif yaklaşımlar geliştirmelidirler.

Güvenlik uzmanlarının karşılaştığı en büyük sorun, bu sistemler arasında güvenliği tutarlı bir şekilde yönetmek ve denetleyebilmektir. Şifre uzunluğu, son kullanma tarihi ve format gibi bireysel güvenlik politikaları her bir platformda farklı formatlarda saklanmalıdır.

Kurumlar bilişim sistemlerini kuracak, kullanacak, denetleyecek personele yatırım yapmalı ve personel politikalarını tekrar gözden geçirmelidir. Bunun yanısıra yöneticilerde güvenlik politikaları konusunda eğitilmelidir.

Bilgi güvenliği yönetim sistemi (BGYS), kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas

bilginin korunmasıdır [Önel ve Dinçkan, 2007]. Kurumlarda mutlaka bilgi güvenliği yöneticisi olmalıdır. Bu personelin görevleri arasında güvenlik politikalarını oluşturmak ve yönetim tarafından onaylanmasını, kurum çalışanları tarafından benimsenmesini sağlamak, kurum güvenlik politikalarının güncelliğini ve sürekliliğini sağlamak, bilgi sistemlerinin güvenlik politikalarına uygunluğunun kontrolünü yapmak, kurum çalışanlarının güvenlik politikalarına uymasının denetlenmesini yürütmek gibi görevleri olmalıdır. Düzenli ve kısa süreli eğitimlerde güvenlik politikasının gerekçeli sunumu yapılmalı, tehditlerin ve sonuçlarının vurgulandığı anlatımlar kullanılmalıdır.

6. KAMU KURUM VE KURULUŞLARINDA ELEKTRONİK İMZA KULLANIMI VE UYGULAMALARI

Bilginin güvenliği kadar kime ait olduğu da önemlidir. Elektronik posta ile alınan bir belgenin gerçekten kime ait olduğunu ispatlanamadığı sürece o belge hiçbir değer taşımamaktadır. Kağıt üzerine yazılı metinlerin ve belgelerin en önemli unsurlarından biri olan imza, bilişim sektöründeki hızlı gelişmeler sonucu günümüzde elektronik metinlerde yer almaktadır. Temel olarak elektronik metinlerin güvenliğinin sağlanması fikri ile ortaya çıkan e-imza, güvenlik kaygıları ile birlikte kimlik bilgisi, zaman bilgisi, inkar edilememezlik ihtiyaçlarına cevap verebilen tek uygulamadır.

Birçok bilgi, veri ve belgenin içerikleri kadar güvenlikleri de önem kazanmaktadır. Son derece önemli bu bilgiler elektronik imza ile korunacaktır. Elektronik imza yasal temeller üzerine oturtularak kullanılma aşamasına getirilmiştir.

6.1. E-imza Kullanımında Açık Anahtar Altyapısı

5070 sayılı kanuna göre elektronik imza "elektronik veriye eklenen veya elektronik veriyle bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir" [5070 Sayılı Elektronik İmza Kanunu]. Şifreleme, elektronik ortamda iletilen bilginin dönüştürülmesi işlemidir. Bu yöntemde bilgi, alıcı dışında başka bir kişi tarafından okunamaması ya da değiştirilememesi için kodlanır. Şifreleme ile gönderilen herhangi bir bilginin gizliliği korunmuş ve bütünlüğü bozulmamış olur. Şifreleme yönteminde güvenliği artırmak amacıyla çeşitli şifreleme algoritmaları kullanılmaktadır. Elektronik imza uygulamalarında kullanılan en yaygın kullanılan yöntem açık (simetrik olmayan) anahtar algoritmasıdır.

Açık anahtar alt yapısı (AAA) birçok kaynakta "bilgi iletişiminde açık anahtarlı şifrelemenin yaygın ve güvenli olarak kullanılabilmesini sağlamaya yarayan ve birbirleriyle eşgüdüm içinde çalışan anahtar üretimi, anahtar yönetimi, onay kurumu, sayısal noterlik, zaman damgası gibi hizmetlerin tümü" şeklinde tanımlanmaktadır.

Ana amacı; sanal dünyada; herhangi bir bilgi taşınırken Gizlilik, Bilgi Bütünlüğü, Kimlik Doğrulama ve Gönderenin İnkar Edememesi güvenlik özelliklerinin sağlanması olan AAA; bu işlemleri Sayısal İmza ve Sayısal şifre ile Özel ve Genel anahtar kullanarak gerçekleştirmektedir. Sayısal imza; Kimlik Doğrulama, Bilgi Bütünlüğü ve Gönderenin inkar edememesi; Sayısal şifre ise Gizlilik güvenlik fonksiyonlarını sağlamaktadır.

AAA kullanıldığı durumda, açık anahtar genellikle veritabanlarından yayınlanır ve isteyen herkes istediği kişinin elektronik sertifikasını okuyarak açık anahtarını öğrenebilir. Gizli anahtar ise sadece kullanıcının kendisi tarafından bilinir ve kullanılır [Genç, Gebze İleri Teknoloji Üniversitesi].

Bir anahtarın diğerinden türetilmesi veya hesaplanması mümkün değildir. Açık anahtarın başkaları tarafından bilinmesinin bir sakıncası yoktur fakat gizli anahtar kesinlikle bir başkası bilmemelidir. Dijital anahtarlar açık-gizli anahtar şifreleme algoritması üzerine kurulmuştur. Bir açık-gizli anahtar çifti bir sayı çiftinden ibarettir. Gizli anahtar sadece sahibi olan kişi ya da kurum tarafından bilinir ve dijital imzayı oluşturmak için kullanılır. Açık anahtar ise dijital imzaların doğrulanması için kullanılır. Bir dijital imzanın doğrulanması mesajın geldiği kişinin kimliğinin doğrulanması anlamına gelmektedir.

6.2. Sayısal-Elektronik İmza

İmza, bir yazının kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla metnin altına konulan isim veya işarettir. İmza, bir yandan kişinin hüviyetini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece imzalayanın metni okuyup anladığı ya da belgeyi bizzat hazırlayan kişi olduğu anlaşılır [2004/21 Kamu sertifikasyon merkezi oluşturulması hakkında, Başbakanlık genelgesi].

Sayısal imzanın işlevi, elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal dokümanların olduğu şekilde, herhangi bir tahrip ve tahrifata uğramaksızın iletilmesini sağlamaktır. Bu nedenle sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir denilebilir.

6.3. E-İmza Tekniği

E-imza, "kişinin elle attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştiren matematiksel formüllere ve şifreleme programlarına verilen isimdir" Çift anahtarlı şifreleme yöntemini kullanarak bilginin bozulmamış/ bütün olduğunu ve gönderenin kimliğini ispatlamak için atılan sayısal imza şunlara bağlı olarak oluşturulur. Gönderilen bilginin sayısal içeriği yani bilgisayarda sıfır/bir dizisi halinde gösterimi ve gönderenin gizli anahtarı.

Bilginin gizliliğini sağlayacak olan şifreleme işlemi ise bilginin sayısal içeriğine ek olarak bilgiyi alacak olan kişinin kamuya açık anahtarını kullanarak yapılır. Sayısal imzanın doğruluğunu kanıtlamak için mesajı alan taraf kendisine gelmiş olan mesajın (ya da bilginin) sayısal içeriğini ve gönderen tarafın açık (ya da kamuya açık) anahtarını kullanır.

6.4. Zaman Damgası

Günlük yapılan işlerde, karışıklığa sebebiyet vermemek için yapılan işlemlerden birisi de, işlemlerin çoğunda tarih bilgisi kullanmaktır. Eğer kullanılmaz ise, işlemlerde, haberleşmede, ilişkilerde ve işlerde problemler çıkabilmekte, kişiler zarar görmekte ve kurumlarda kayıplar oluşabilmektedir.

E-imzanın kullanıldığı tarih zaman damgası ile ispat edilebilir. Ancak, imzanın geçerli olabilmesi için imzanın atılmış olduğu TÜBİTAK tarafından e-imza sahibine verilen ve e-imza yetkisi sağlayan sertifikanın da bu tarihte geçerli olduğunun ispatı gerekmektedir.

6.5. E-İmzanın Özellikleri

Yazılı dokümanlarda kullandığınız imzalar gibi, e-imzalar da günümüzde e-posta veya elektronik verilerin yazarlarını/sahiplerini tanılamada kullanılmaktadır. Elektronik imzalar, elektronik sertifikalar kullanılarak yaratılır ve doğrulanırlar. Bir bilgiyi imzalamak, güvenli bir alışverişi gerçekleştirmek için kendi özel Elektronik sertifikanıza ihtiyaç vardır.

E-imzanın kullanımın dünya çapında kabul görmesinin ve gittikçe yaygınlaşmasının sebepleri şöyle sıralanabilir.

- E-imza güvenilirdir,
- E-imza taklit edilemez,
- E-imza yeniden kullanılamaz,
- E-imzalı metin değiştirilemez ve
- E-imza inkar edilemez.

6.6. Veri bütünlüğü ve gizlilik

E-imzalar verinin bütünlüğünü koruyarak okuduğunuz mesajın, kazayla veya kötü niyetle size gelene kadar değişmediğini veya değiştirilmediğini garanti eder. Teknik olarak anlatmak gerekirse, sayısal olarak imzalanan dokümanın hash denilen küçük bir özü tutulur. İmzalama işleminin ardından dokümanda yapılacak herhangi bir değişiklik, bu sayısal özü farklı yani geçersiz kılacaktır. Verinin gizliliği, alıcının açık anahtarının mesajı şifrelemede kullanılması sayesinde gerçekleştirilir.

7. DÜNYADA VE TÜRKİYE'DE ELEKTRONİK İMZA ALTYAPILARI VE UYGULAMALAR

7.1. Dünyada e-İmzaya Geçiş

Dünyada 1996 yılında, ülkemizde 2004 yılında hazırlanan mevzuatlarla hukuki altyapısı belirlenmeye başlanan e-imza, halihazırda birçok ülkede yasal olarak uygulanmaya başlamıştır. E-imza, Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu(UNCITRAL) tarafından, 1996 yılında Elektronik Ticaret Model Yasası'nın ve 2001 yılında Elektronik İmza Model Yasası'nın çıkarılmasıyla, dünya ülkelerince gerekli hukuki düzenlemeler yapılarak uygulamaya geçirilmeye başlanmıştır. Avrupa Birliğine uyum süreci Türkiye'de e-imza altyapısının oluşmasına temel teşkil etmiştir.

7.2. Türkiye'de E-İmza Oluşumu ve Uygulamaları

Elektronik İmza Kanun Tasarısı, 15 Ocak 2004 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş, Kanun, 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmıştır. İkincil düzenleme çalışmaları Telekomünikasyon Kurumu'na verildiğinden, Kanunun verdiği 6 aylık zamandan önce ikincil mevzuat çalışmaları tamamlanarak yürürlüğe girmiştir. Mevzuat çalışmalarının ardından elektronik imzanın uygulamaya girmesi için gerekli çalışmalar başlamıştır.

Elektronik imzanın kamu kurumlarında otomasyonu sağlayacak şekilde yaygınlaştırılması ve özel sektörde elektronik ortamda verilen çeşitli belgelerin e-imza ile yasal geçerliliğinin sağlanması amaçlanmaktadır. Son olarak ise siber alandaki güvenlik tehditlerini takip edecek ve risklerin ortaya çıkması durumunda müdahale edecek bir Bilgisayar Acil Durum Tepki Ekibi'nin (BADTE) kurulması Önerilmektedir.

7.3.Kamu Kurumlarında E-imza Uygulamaları

Uygulamalar açısından Türkiye'deki mevcut duruma bakıldığında; kurumsal işlemlerin ve vatandaşa yönelik hizmetlerin elektronik ortama aktarılmakta olduğu, bu anlamda kamu sektöründe birbirinden bağımsız çalışmalar yapıldığı, kurumların bilgi verme amaçlı olarak anakapı oluşturduğu, ancak henüz bu anakapılar üzerinden elektronik işlem yapılması çalışmalarının henüz başlangıç aşamasında olduğu görülmektedir.

7.4. Türkiye'de İnternet Kullanımı

Türkiye internet sektörü raporuna göre, Türkiye'nin internet kullanıcısı sayısı 26 milyondur. Bu sayı ile Türkiye dünyanın 11**.** en büyük internet popülasyonu haline gelmiştir. Türkiye'deki internet penetrayonu %37 dir. Bu sayı Avrupa ortalaması olan %59 ile kıyaslandığında oldukça değerli bir aşamayı oluşturuyor. Kasım 2006 sayıları ile Türkiye'de 7.5 milyon geniş bant internet kullanıcısı bulunmaktadır. Bu sayı ile Türkiye dünya çapında 9. ülke konumunda yer almaktadır. Türkiye'de 2009 yılında yaklaşık $9 milyar bir elektronik ticaret hacmi ve pazarı bekleniyor [Kutsal, 2008].

Türkiye e-devlet uygulamaları açısından dünya sıralamasında %43,5 ile 9. sırada yer almaktadır. Türkiye internet kullanıcılarının %45,03 gibi büyük bir bölümü 16-24 yaş aralığındadır. Bunun yanında internet kullanıcılarının %66'sı erkek, %34'ü kadın olarak tespit edilmiştir. Kullanıcıların %22'si üniversite mezunu, %68'i bekar, %45'i çalışıyor, %39'u İngilizce biliyor, %52'sinin evinde bilgisayar var, %91'inin cep telefonu var, %84'ü günlük olarak ortalama 3 saat televizyon seyrediyor, %63'ü günlük olarak ortalama 2 saat radyo dinliyor, kullanıcılar günlük olarak ortalama 2,5 saat internete bağlı kalıyorlar. 2010 yılında Türkiye de internet kullanıcı sayısı 32-36 milyon olması beklenmektedir [Kutsal, 2008].

Türkiye İstatistik Kurumunun araştırma sonuçlarına göre, son üç ay içerisinde İnternet kullanan bireylerin % 75,9'u gazete ya da dergi okumak, % 73,6'sı e-posta göndermek-almak, % 69,3'ü anlık ileti göndermek (Chat, Msn, Skype, başkaları ile gerçek zamanlı yazışma), % 64,4'ü müzik indirmek ya da dinlemek (web radyo hariç) için İnterneti kullanmıştır [Türkiye İstatistik Kurumu, 2009].

7.5. Dünyada internet kullanımı

"Internet Worldstats"ın, araştırma şirketi ACNielsen'e dayanarak yayımladığı verilere göre, halen dünyada yaşayan 6 milyar 420 milyon insanın yüzde 13,9'u (938 milyon 711 bini) internet kullanıyor. Son 4,5 yılda dünyada internet kullanıcılarının sayısı yüzde 160 arttı. Fakat bu oran Türkiye'nin de içinde bulunduğu Ortadoğu'da yüzde 312, olarak gerçekleşti. Ülkelere bakıldığında ise yaklaşık 203 milyon ile dünyada en fazla internet kullanıcısına sahip ABD'yi 103 milyon internet kullanıcısıyla Çin, 78 milyon internet kullanıcısıyla Japonya ve 47 milyon internet kullanıcısıyla Almanya izlemektedir [http//www.internetworldstats.com].

Türkiye kullanıcı sayısının nüfusa oranı bakımından % 9,9 oranla alt sıralarda yer almaktadır. Özellikle internet erişiminin dünyanın bir çok ülkesi ile karşılaştırıldığında son derece pahalı olması en önemli etkenlerden olduğu değerlendirilmektedir.

8. ARAŞTIRMANIN YÖNTEMİ

Tez çalışmasının bu kısmında Türkiye'deki kamu kurum ve kuruluşlarında bilgi veri ve sistem güvenliğine ilişkin yapılan alan araştırmasının yöntem bilgileri verilip, istatistiksel analizleri gerçekleştirilecektir.

8.1. Araştırmanın Kapsamı

Araştırma Türkiye'deki kamu kurum ve kuruluşlarının bilgi işlem merkezlerini kapsamaktadır.

8.2. Araştırmanın Örnekleminin Belirlenmesi

Türkiye'deki Kamu kurum ve kuruluşlarının bugün itibariyle büyük bir kısmı tüm alt birimlerinin de bağlı olduğu ve merkezi bilgi işlem ünitesinin Bakanlık, Başkanlık, Genel Müdürlük vb. bünyesinde bulunduğu bir yapıya sahiptir. Merkezi idareye bağlı kurum ve kuruluşların bazı istisnaları hariç tamamına yakını Ankara'da bulunmaktadır. Bunların hem merkez teşkilatlarında hem de yerel teşkilatlarında bilgi işlem faaliyeti yürütülmektedir. Yerel birimlerin bilgi işlem faaliyetleri de merkez birimlerin bilgi işlem merkezleri tarafından koordine edilmekte, ya da doğrudan merkez bilgi işlem merkezlerine bağlı olarak çalışmaktadır. Dolayısıyla, yerel birimlerdeki bilgi ve sistem güvenliğine ilişkin mevcut durumu ve güvenlik politikalarını, merkez birimlerdeki mevcut durum, sorun ve politikalardan ayrı düşünmemek gerekir. Ankara dışındaki bazı birkaç Genel Müdürlük, üniversiteler, yerel yönetimler ve hastaneler bu istisnalar arasında yer almaktadır. Böylece, Ankara'da mevcut olan bilgi işlem merkezleri genel idareye ait bilgi işlem merkezlerinin iyi bir temsilini sağlar. Bu nedenle araştırmanın örneklemini Ankara'da kamu kurum ve kuruluşları oluşturmuştur. Yerel yönetimler ve üniversiteleri temsil etmek üzere yine Ankara'da buluna dört belediye bilgi işlem merkezi ve bir üniversite örnekleme dahil edilmiştir. Bu nedenle, bu araştırmanın

örneklemi Ankara'daki kamu kurum ve kuruluşlarından kota örneklemesi ile belirlenmiştir.

Öncelikle, Ankara'da yerleşik kamu kurum ve kuruluşların bir listesi oluşturulmuştur. Çerçevenin oluşturulması aşamasında Başbakanlık tarafından hazırlanmış ve tüm kamu kurum ve kuruluşlarını içeren bir çalışmadan yararlanılmıştır. Daha önce kamu kapsamına ait olup, özelleştirme nedeniyle özelleştirilen ve özelleştirme kapsamına alınan kuruluşlar bu listeden çıkarılmıştır. Böylece Ankara'da bulunan merkezi idareye bağlı toplam 120 kamu kurum ve kuruluşunun tamamına ulaşılması hedeflenmiştir. Üniversite ve belediyeler bu listenin içinde yer almamaktadır.

Araştırmanın örneklemini belirlemek için önceden bir örneklem büyüklüğü belirlenmemiştir. Merkezi idareye bağlı 120 kurum ve kuruluşun yanı sıra Ankara'daki tüm belediye ve üniversitelerin tamamına da ulaşılması hedeflenmiştir. Böylece, gözlem birimlerinin örneğe çıkması tesadüfi örnekleme ile değil kota örneklemesi ile belirlenmiştir.

8.3. Anketin Cevaplanma Oranı ve Cevap Kalitesi

Hazırlanan anket 120 merkezi idareye bağlı kamu kurum ve kuruluşunun yanı sıra dört devlet üniversitesi ve yedi belediye bilgi işlem merkezine ulaştırılmış, ancak bunlardan 82 tanesinden cevap alabilmek mümkün olmuştur. 49 kurum ve kuruluş yöneltilen soruların cevaplanmasının idari sorun yaratacağı endişesiyle ankete katılmak istememiştir. Bu türden verilerin gizliliği konusundaki duyarlılığın sözkonusu olduğu bir araştırmada ulaşılan %62.5'lik cevaplama oranı oldukça başarılı ve analizleri yapmaya elverişli bir orandır.

Ankete katılan kurumların niteliklerine göre dağılımı şöyle olmuştur:

Çizelge 8.1. Ankete katılan kurumların niteliklerine göre dağılımı

Kurumun Niteliği	Kurum veya Kuruluş sayısı
Bakanlık	16
Genel müdürlük	23
Üniversite	3
Belediye	4
Yargı kurumları	6
Kurul ve Başkanlık	27
Banka	2
Hastane	1

Ankette yöneltilen bilgi işlem merkezleri bütçeleriyle ilgili olanlar hariç tüm sorulara yüksek bir oranla cevap almak mümkün olmuştur. Bu nedenle, bütçe boyutuna ilişkin sonuçlar elde edilememiştir.

8.4. Anket Formunun Geliştirilmesi

Anket formu birkaç aşama halinde yapılan çalışma sonunda geliştirilmiştir. Öncelikle, bazı kamu kurum ve kuruluşu bilgi işlem merkezleri ziyaret edilerek, sorumlu ve uzman kişilerle, bilgi işlem merkezlerine yönelik donanımsal, fiziksel, güvenlik, saldırılar, tedbirler vb. konularda nitel görüşmeler yapılmıştır. Bu görüşmeler, anket formundaki soruların belirlenmesinde önemli girdiler sağlamıştır.
İkinci görüşme ise, kamu kurum ve kuruluşları ile çalışan profesyonel bilgi güvenliği alanında faaliyet gösteren firmalar ile yapılmıştır. Firmalarla yapılan görüşmelerde dışarıdan kamunun ihtiyaçlarını tespit etme ve bu ihtiyaçları temin etme zorlukları konusunda bilgi edinilmiştir. Çalışmadan bahsedilerek, ne türden soruların yöneltilebileceği konusunda görüş alınmıştır.

Üçüncü aşamada, hazırlanan soru formu kamu bilgi işlem merkezlerindeki bazı uzman kişilerle yüz yüze tartışılmış ve uzman görüşü çerçevesinde yöneltilmesi anlamlı olabilecek 75 sorudan oluşan soru envanterinin son hali oluşturulmuştur. Son aşamada ise, hazırlanan anket formu, bir pilot çalışma çerçevesinde beş kurumda yüz

yüze uygulanarak, anlaşılma zorlukları, anlam farklılıkları yaratma, cevaplama zorluğu vb. hususlar bakımından eksiklikleri tespit edilmiştir.

Bu ön çalışmaların sağladığı girdiler dikkate alınarak, çalışmanın anket formundaki soruların, tematik biçimde altı grupta toplanmasına karar verilmiştir. Soru grupları aşağıdaki tematik başlıklarda sınıflandırılmıştır.

Çizelge 8.2. Anket sorularının temasına göre dağılım

Tema	Soru Grubu	Soru Adedi
Bilgi işlem birimlerinin idari yapısı ve personel profili	A	7
Bilgi işlem birimlerinin internet hizmetleri	B	8
Bilgi işlem birimlerinin donanım alt yapısı	C	10
Bilgi işlem birimlerinin güvenlik hizmetleri	D	35
Bilgi işlem birimlerinin bakım ve teknik destek	E	9
Bilgi işlem birimlerinde çalışanların memnuniyeti	F	6

Uygulanan anket formu EK-1'de verilmiştir.

8.5. Anketin Uygulanması

Hazırlanan anket formu kurum ve kuruluşlarda genellikle iki gruptan kişiye uygulanmıştır. Yönetim boyutu ile ilgili sorular yönetici pozisyonundaki kişilere, teknik boyuttaki sorular ise eğer yönetici tarafından cevaplanamıyorsa teknik uzman statüsündeki kişilere yöneltilmiştir.

Anketin uygulanmasında, kurum veya kuruluş bilgi işlem yöneticisinden önceden randevu alınmıştır. Kurum ve kuruluşlar ya araştırmacının kendisi tarafından ya da çalışmada istihdam edilen iki profesyonel anketör tarafından gerçekleştirilmiştir. Mümkün olduğunca anket sorularına bu ziyaret esnasında cevap verilmesi sağlanmış, mümkün olmadığı durumlarda ise daha sonra cevaplanmak üzere anket formu kendilerine bırakılmıştır.

Deneklerden dönen formlar incelenip, ilgili birimler aranarak cevap verilmeyen sorulara da cevap verilmesi sağlanmıştır.

8.6. Araştırmanın İstatistiksel Analiz Yöntemleri

Anket çalışmasından elde edilen verilerin girişleri ve analizler SPSS 18 ortamında gerçekleştirilmiştir. İstatistiksel analizler, her bir değişkene ilişkin frekans tabloların oluşturulması, değişkenler arası ilişkilerin araştırılmasında ki-kare bağımsızlık testi ve örneklem birimlerinin tematik alanlar itibariyle benzerliklerine/ayrışmalarına ilişkin olarak da kümeleme analizi yapılması biçiminde gerçekleştirilmiştir.

8.6.1. Frekans tabloları

Frekans tabloları veriyi özetlemenin en etkin yollarından birisidir. Sınıflama düzeyinde ölçülmüş araştırma değişkenlerinin frekans dağılımlarına, birikimli frekans dağılımlarına ve oransal frekans ve birikimli oransal frekans dağılımlarına ilişkin bilgiler frekans tablolarıyla elde edilmiştir.

8.6.2. Pearson Ki-kare ilişki analizi

Pearson Ki-kare istatistiği frekans tablosu biçimindeki satır ve kolon nitel değişkenleri arasındaki "ilişki yoktur" hipotezinin testi için kullanılır. Ki-kare istatistiği her bir gözenin gözlenen frekansı ile teorik frekansı arasındaki farkın karelerinin teorik frekansa bölünmesiyle elde edilen değerler toplamı biçiminde tanımlanır. Test istatistiği Ki-karenin hesaplama formülü aşağıdaki gibi yazılır.

$$\sum_{i=1}^{I}\sum_{j=1}^{J}\frac{(O_{ij}-E_{ij})^2}{E_{ij}} \sim \chi^2 \qquad (8.1)$$

Burada, O_{ij}:gözlenen ferkans, E_{ij}:beklenen (teorik) frekans olarak tanımlıdır.
Teorik frekanslar ise aşağıdaki gibi hesaplanır.

$$E_{ij} = \frac{(R_i)(C_j)}{n} \tag{8.2}$$

Burada kullanılan simgelerin tanımı şöyledir.

R_i: satır nitel değişkeninin i nci düzeyine karşılık gelen satır toplamı
C_j: kolon nitel değişkeninin j nci düzeyine karşılık gelen kolon toplamı
n: örneklem büyüklüğü

İki değişken birbirinden bağımsızdır biçiminde tanımlanan yokluk hipotezinin doğruluğu altında belli koşullar sağlandığında χ^2 istatistiği χ^2_{sd} olasılık dağılımına sahiptir. $sd = (r-1)(c-1)$, r, satır değişkeni düzey sayısını, c, kolon değişkeni düzey sayısını göstermektedir.

α anlamlılık düzeyi ve χ^2_h de bu istatistik için hesaplanan değer $\Pr(\chi^2_{sd} > \chi^2_h) < \alpha$ ise iki değişken bağımsızdır biçimindeki yokluk hipotezi reddedilir.

8.6.3. İki aşamalı kümeleme analizi

Kümeleme analizi, bir veri kümesindeki gözlemlerin (ya da değişkenlerin) değişkenler bakımından birbirine benzer olanlarını bir arada gruplandırmada kullanılan çok değişkenli istatistik analiz yöntemlerinden birisidir.

K-ortalamalar ya da hiyerarşik kümeleme algoritmaları değişkenlerin sürekli türden olmasını gerektirir. Değişkenlerin niteliksel kesikli türden olduğu durumlarda her iki yöntem de uygun yöntemler değildir. Değişkenlerin multinomial ya da multinomial ve sürekli değişkenlerin her ikisinin de olduğu durumlarda kullanılabilecek uygun bir yöntem "iki aşamalı kümeleme"dir. SPSS istatistiksel analiz yazılımındaki iki aşamalı kümeleme algoritması, Banfield ve Ratfery tarafından önerilen iki küme birleştirildiğinde log-likelihood'daki azalmaya dayalı sürekli değişkenler için

kümeleme algoritmasının ve Melia ve Heckerman'in kategorik değişkenler için benzer olasılıklı yaklaşımının geliştirilmiş bir uzantısıdır. Bu algoritmanın aşamaları şöyle özetlenebilir [Banfield ve Ratfery, 1993], [Melia ve Heckerman 1998].

Adım 1: Ön kümeleme_küçük kümeler oluşturma

Birinci adım ön kümelerin oluşturulmasıdır. Ön kümelemede amaç, tüm mümkün gözlem çiftleri arasındaki uzaklıkları içeren matrisin boyutunu indirgemektir. Ön kümeleme aşaması ardışık bir yaklaşım kullanır. Algoritma uzaklık ölçüsüne dayanarak, ya gözlemi önceki ön kümelere ekler ya da yani bir küme başlatır. Ön kümeleme tamamlandığında, aynı ön kümedeki tüm gözlemler tek bir veri gibi gözlem gibi değerlendirilir. Uzaklık matrisinin büyüklüğü artık gözlem sayısına değil, ön kümelerin sayısına bağımlıdır.

Adım 2: Ön kümelerin hiyerarşik kümelemesi

Bu aşamada, algoritma bilinen hiyerarşik kümeleme algoritmasını kullanır. Kümelerin oluşturulmasında log-likelihood uzaklık ölçüsü kullanılır. Gözlemler kümelere en büyük log-likelihood değerlerine göre atanırlar.

SPSS iki aşamalı küme algoritmasında optimal kümelerin belirlenmesinde iki aşamalı yöntem kullanır. Birinci aşamada her bir küme sayısı için BIC (Schwarz Bayesian kriteri) ya da AIC (Akaike bilgi kriteri) hesaplanır ve böylece küme sayısının bir tahmini elde edilir. İkinci aşamada, her bir hiyerarşik kümeleme aşamasındaki en yakın iki küme arasındaki en büyük artış bulunarak başlangıç tahmin düzeltilir.

J küme için AIC ve BIC aşağıdaki gibi tanımlanır.

$$BIC(J) = -2\sum_{j=1}^{J} \xi_j + m_j \qquad (8.3)$$

$$AIC(J) = -2\sum_{j=1}^{J} \xi_j + 2m_j \tag{8.4}$$

Bu formüllerde $m_j = J\left\{2K^A + \sum_{k=1}^{K^B}(L_k - 1)\right\}$,

K^B kategorik değişkenlerin sayısı, K^A sürekli değişkenlerin sayısı, L^k ise k'ncı kategorik değişkenin kategori sayısını göstermektedir.

SPSS ön kümeleme ve kümeleme aşamalarının her ikisi için de uzaklık ölçüsü kullanır. Log-likelihood uzaklık, uzaklık değerine dayalı olasılıktır. İki küme arasındaki uzaklık ikisi bir kümede birleştirildiğindeki log-likelihood'daki azalmayla ilişkilidir. *j* ve *s* kümeleri arasındaki uzaklık şöyle tanımlanır.

$$d(j,s) = \xi_j + \xi_s - \xi_{<j,s>} \tag{8.5}$$

Burada,

$$\xi_j = -N\left(\sum_{k=1}^{K^A}\frac{1}{2}\log(\hat{\sigma}_k^2 + \hat{\sigma}_{jk}^2) + \sum_{k=1}^{K^B}\hat{E}_{jk}\right) \tag{8.6}$$

$$E_{jk} = \sum_{l=1}^{L_k}\frac{N_{jkl}}{N_j}\log\frac{N_{jkl}}{N_j} \tag{8.7}$$

olarak tanımlıdır.

$\hat{\sigma}_k^2$ k'ncı sürekli değişkenin tüm veri için varyans tahminini, $\hat{\sigma}_{jk}^2$ j'nci kümedeki k'ıncı değişken varyans tahminini, N_{jkl} k'ncı kategorik değişken için l kategori değerini alan j'nci kümedeki gözlem sayısını, N_j ise j'nci kümedeki gözlem sayısını

göstermektedir. Eğer $\hat{\sigma}_k^2$ eşitlikte ihmal edilecek olursa, *j* ve *s* kümeleri arasındaki uzaklık, iki küme birleştirildiğinde log-likelihood'da azalma meydana gelir. $\hat{\sigma}_k^2$ terimi, bir kümede tek gözlem olduğunda doğal logaritma teriminin tanımsız olacağı $\hat{\sigma}_{jk}^2 = 0$ durumunu önlemek için eklenir.

9. ARAŞTIRMANIN BULGULARI

Çalışmanın bu kısmında yapılan istatistiksel analizler ve bulgular verilerek yorumlanacaktır. Her bir çizelgenin başlık kısmında parantez içerisinde, anket formundaki karşılık geldiği soru numarası verilmiştir.

9.1. İdari ve Fiziksel Alt Yapı

Bu kısımda A grubu sorulara ilişkin dağılımlar verilip sonuçlar irdelenecektir.

Çizelge 9.1. BİM'lerin idari yapısına göre dağılımı (A-1)

BİM idari yapıları	Kurum Sayısı	%
BİM Genel Md.	2	2,4
BİM Başkanlığı	3	3,7
BİM Daire Bşk	34	41,5
BİM Müdürlüğü	8	9,8
BİM Şube Müd.	15	18,3
BİM Merkezi	6	7,3
BİM Şefliği	3	3,7
Diğer	11	13,4
Toplam	82	100,0

Kamu kurumlarında idari yapı olarak bilgi işlem faaliyetleri, %41,5 oranla en çok Daire Başkanlığı olarak yürütülmektedir. Az sayıda ise Genel Müdürlük ve BİM şefliği olarak örgütlendiği gözlenmiştir. Kamu kurumları idari örgütlenme bakımından belli bir standarda sahip değildir.

Çizelge 9.2. Kurumların aktif kullanıcı sayısının dağılımı (A-2)

Kullanıcı sayısı	Kurum sayısı	%	Birikimli%
50-100	4	4,9	4,9
100-500	25	30,5	35,4
500-1000	14	17,1	52,4
1000-+	39	47,6	100,0
Toplam	82	100,0	

Kurumların %47,6'sının kullanıcı sayısı 1000 kullanıcının üzerinde iken geri kalan kısmı 1000 ve daha az sayıda kullanıcıya sahiptir. 50-100 kullanıcı arasında değişen küçük ölçekli kurum oranı %4,9 dur.

Çizelge 9.3. BİM'lerin çalışan personel sayısına göre dağılımı (A-3)

Personel sayısı	Kurum sayısı	%	Birikimli %
1-9	15	18,29	18.29
10-30	35	42,68	60.98
31-60	17	20,73	81.71
61-100	8	9,76	91.46
101-200	4	4,88	96.34
200-+	3	3,66	100.00
Toplam	82	100.00	

BİM'lerin %42,68'inde çalışan sayısı 10-30 kişi ile en yüksek çalışan grubu oluşturmaktadır. BİM'de çalışan sayısı 200 den fazla olan kurumların oranı ise sadece %3,66'dır.

Çizelge 9.4. BİM'de çalışanların eğitim durumlarına göre dağılımı (A-4)

Eğitim durumu	Çalışan sayısı	%
İlköğretim	9	0
Lise	293	9
Ön lisans	581	17
Lisans	2327	67
Y.Lisans	204	6
Doktora	20	1
Toplam	3434	100

BİM'lerinde çalışanların büyük çoğunluğu %67 oranıyla lisans mezunudur. Çalışanların büyük kısmı lisans ve lisansüstü eğitime sahip kişilerden oluşmaktadır. Çalışanların %1'lik kısmının doktora eğitimine sahip olduğu gözlenmiştir.

Çizelge 9.5. BİM'lerin bilgisayar ve bilgisayar güvenliği eğitimine göre dağılımı (A-5)

Eğitim Durumu	Kurum sayısı	%
Eğitim verildi	53	64,6
Eğitim verilmedi	29	35,4
Toplam	82	100,0

BİM'de çalışanlara en az bir defada olsa eğitim veren kurumların oranı %64,6 dır. Hiç eğitim verilmeyen kurumların oranı oldukça yüksek olarak değerlendirilebilir. Eğitim eksikliği, sistem ve veri güvenliği bakımından önemli açıklar oluşmasının anlamlı nedenlerinden birisi olabilir.

Çizelge 9.6. BİM'lerin bilgisayar ve bilgisayar güvenliği eğitiminde verilen eğitimlerin sıklığına göre dağılımı (A-6)

Eğitim sıklığı	Kurum sayısı	%	Birikimli %
Sıklıkla	6	11,3	11,3
Arasıra	23	43,4	54,7
Nadiren	19	35,8	90,5
Diğer	5	9,4	100,0
Toplam	53	100,0	

Eğitim verilen kurumların %43,4'ü arasıra (yılda bir defa) eğitim verirken, %35,8'i nadiren (iki yılda bir defa) eğitim vermektedir. Eğitim veren kurumların da bu eğitimleri olması gereken sıklıkta vermediği görülmektedir.

Çizelge 9.7. Kamu Bilgi İşlem birimlerinde eğitim türlerine göre sıklık dağılımı (A-7)

Eğitim türleri	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
PC güvenliği	31	21,7	58,5
Bilgisayar temel eğitimi	34	23,8	64,2
Ofis programları eğitimi	30	21,0	56,6
İleri düzey kullanıcı eğitimi	25	17,5	47,2
Teknisyenlik eğitimi	11	7,7	20,8
Diğer	12	8,4	22,6
Toplam	143	100,0	

Eğitim alan kurumların aldıkları eğitim türleri içinde en yüksek oranı %64,2 ile bilgisayar temel eğitimi oluşturmaktadır. Kurumların yarısından biraz fazlasının ise PC güvenliği konusunda eğitim aldığı görülmektedir. Alınan tüm eğitimler içinde en yüksek payı PC güvenliği, bilgisayar temel eğitimi ve ofis programları eğitimi oluşturmaktadır. Bilgi ve sistem güvenliği konusunda alınacak tedbirlerin içinde önemli bir unsur olan kullanıcıların bu konuda bilinçlendirilmesi, kurumların yarısına yakın kısmında faaliyet olarak gerçekleştirilmemiş olup, bu durum ciddi potansiyel tehlike kaynaklarından birisidir.

9.2.İnternet Altyapısı ve Bakım

Bu kısımda internet altyapısı ve bakıma ilişkin B grubu soruların sıklık dağılımları verilmiştir.

Çizelge 9.8. Kurumların internet hizmeti verme durumuna göre dağılım (B-8)

İnternet hizmeti	Kurum sayısı	%
İnternet hizmeti veriliyor	80	97,6
İnternet hizmeti verilmiyor	2	2,4
Toplam	82	100,0

Kurumların %97,6 gibi büyük bir bölümünün internet çıkışının bulunduğu ve çalışanlarına internet hizmeti sunduğu görülmektedir.

Çizelge 9.9. İnternet bağlantı türlerine göre dağılım

İnternet bağlantı türleri	Cevap sayısı	Cevaplara göre %	Kurumlara göre %
Metro ethernet	74	72,5	92,5
ADSL	20	19,6	25,0
ISDN	1	1,0	1,3
Dial-Up	1	1,0	1,3
X25	1	1,0	1,3
Diğer	5	4,9	6,3
Toplam	102	100,0	127,5

Kurumların %92,5'i internet hizmetini sağlamada Metro ethernet bağlantısına sahiptir. İkinci sırada benimsedikleri ise ADSL bağlantısıdır. Tüm bağlantı türleri içinde ise Metro Ethernet %72,5 orana sahiptir. ADSL bağlantı türünü tercih eden kurumlar, sadece internet hizmeti almak amacıyla tercih etmektedirler.

Çizelge 9.10. İnternet hızlarına göre kurumların dağılımı (B-10)

İnternet hızları (Mb/ps)	Kurum sıklığı	%	Birikimli %
1-10	26	35,6	35,6
11-40	24	32,9	68,5
41-80	15	20,5	89,0
81-160	6	8,2	97,3
160-+	2	2,7	100,0
Toplam	73	100,0	

Kamu kurum ve kuruluşları iş yükünün durumuna göre internet hizmeti alırken, hızını da belirlemektedir. Kurumların %35,6'sı internet çıkış hızını 1-10 Mbps olarak belirlerken %32,9'u 11-40 Mbps arasında hızın yeterli olacağını düşünmektedir. İnternet hızı 160 Mbps den daha fazla olan kurumların oranı ise %2,7 dir.

Çizelge 9.11. Kurumların İnternet hizmetlerinden yararlanması durumuna göre dağılım (B-11)

İnternetten Yararlanma	Kurum sıklığı	%	Birikimli %
Yararlanıyor	75	93.75	93.75
Yararlanmıyor	5	6.25	100.00
Toplam	80	100.00	

Çizelge 9.12. İnternet kullanıcılarının karşılaştığı sorunlara göre dağılımı (B-12)

İnternet kullanıcılarından gelen sorunlar	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
Virüs zaman ve bilgi kaybına neden olması	36	27,3	45,0
Kişisel bilgiler başkalarının eline geçmesi	1	0,8	1,3
Kredi kartı kullanımında zarar görme	4	3,0	5,0
İstenmeyen e-posta ile sık karşılaşma	61	46,2	76,3
Herhangi bir güvenlik sorunu yaşamama	18	13,6	22,5
Diğer	12	9,1	15,0
Toplam	132	100,0	165,0

Çizelge 9.13. Kurumların internet kullanımındaki kısıtlama durmuna göre dağılım (B-13)

İnternet kısıtlaması	Kurum sayısı	%
Kısıt var	4	4.88
Kısıt yok	78	95.12
Toplam	82	

Kurum çalışanlarının %76,3'ü istenmeyen iletilerden (e-posta) rahatsız olduğunu belirtmiştir. Kurum çalışanlarının internet kullanımında karşılaştıkları sorunlar içerisinden en şok şikayet ettikleri %45 oranında virüslerden kaynaklanan zararların olduğu görülmüştür. Her hangi bir problemle karşılaşmayanların oranı %22,5'dir.

Çizelge 9.14.BİM'lerin sürekli yayın takip edilme durumuna göre dağılımı (B-14)

Yayın takip ediliyormu	Kurum sayısı	%
Sürekli yayın takip ediliyor	58	70,7
Sürekli yayın takip edilmiyor	24	29,3
Toplam	82	100,0

Kamu bilgi işlem merkezlerinde (BT) Bilişim teknolojileri ile ilgili güncel yayınların takibini %70'7 oranında yapmaktadırlar. Hangi yolla takip ettikleri Çizelge 1.11 da daha detaylı açıklanmıştır.

Çizelge 9.15. BİM'de sürekli takip edilen yayınların türlerine göre dağılımı. (B-15)

Teknolojik gelişmelerin takibi	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
İnternetten-web	53	29,9	91,4
E-posta yolu ile	46	26,0	79,3
Dergi-Gazeteler	36	20,3	62,1
Televizyonlardan	13	7,3	22,4
Toplantı-seminer	29	16,4	50,0
Toplam	177	100,0	305,2

Bilgi teknolojilerini sürekli yayınlar yolu ile takip eden kurumların en çok kullandıkları araç internet, e-posta ve dergi-gazetelerdir. Bu konuda toplantı ve

seminerler de sıklıkla kullanılan araçlardandır. Tüm cevaplar içinde en yüksek kullanıma sahip bu araçlar %20-30 arası orana sahiptir.

Çizelge 9.16. BİM'nin sunucu sayısına göre dağılımı. (C-16)

Sunucu sayısı	Kurum sıklığı	%	Birikimli %
1-10	19	25,00	25,00
11-30	34	44,74	69,74
31-100	13	17,11	86,84
101-500	10	13,16	100,00
Toplam	76	100,00	

Kurum bilgi işlem merkezlerinde sunucu sayısının %44,74'ünde 11-30 adet aralığında olduğu, %86,84'ünün ise 100 ve daha az sayıda sunucu olduğu görülmektedir.

Çizelge 9.17. Kurumların aktif cihaz sayısına göre dağılım. (C-17)

Aktif sayısı	Kurum sıklığı	%	Birikimli %
1-10	20	28,57	28,57
11-30	27	38,57	67,14
31-100	19	27,14	94,29
101-700	4	5,71	100,00
Toplam	70	100.00	

Kurumların %38,5'inde aktif cihaz sayısının 11-30 adet aralığında olduğu, %94,29'unda ise 100 den daha az olduğu görülmektedir.

Çizelge 9.18. Kurumların masaüstü bilgisayar sayısına göre dağılım(C-18)

Masaüstü bilgisayar sayısı	Kurum sıklığı	%	Birikimli %
1-100	8	10,1	10,1
101-200	10	12,7	22,8
201-500	19	24,1	46,8
501-950	42	53,2	100,0
Toplam	79	100,0	

Kurumların %53,2'sinin masa üstü bilgisayar sayısı 501 ila 950 arasındadır. Ancak kurumların %10,1'inin 1 ile 100 adet bilgisayara sahip olduğu gözlenmektedir.

Çizelge 9.19. Kurumların dizüstü bilgisayar sayısına göre dağılımı. (C-19)

Dizüstü bilgisayar sayısı	Gözlemler	%	Birikimli %
1-100	37	48,7	48,7
101-1000	34	44,7	93,4
1001-10000	4	5,3	98,7
10001-25000	1	1,3	100,0
Toplam	76	100,0	

Kurumların %48,7'sinin dizüstü bilgisayar sayısının 1 ile 100 aralığında, %44,7'sinin 101 ile 1000 aralığında olduğu görülmektedir. Ancak %1,3'ü 10001 ile 25000 arasında yer almaktadır.

Çizelge 9.20. Kurumların yazıcı sayısına göre dağılım. (C-20)

Yazıcı sayısı	Kurum sıklığı	%	Birikimli %
1-10	2	2,7	2,7
11-100	30	40,5	43,2
101-500	24	32,4	75,7
501-800	18	24,3	100,0
Toplam	74	100,0	

Kurumların %75,7'sinin yazıcı sayısı 500 den daha az iken %2,7'sinin yazıcı sayısı 1 ile 10 arasında değişmektedir. %24,3 ünün yazıcı sayısı ise 500 ile 800 arasında değişmektedir.

Çizelge 9.21. Kurumların tarayıcı sayısına göre dağılım. (C-21)

Tarayıcı sayısı	Gözlemler	%	Birikimli %
1-10	28	39,4	39,4
11-100	40	56,3	95,8
101-500	2	2,8	98,6
501-800	1	1,4	100,0
Toplam	71	100,0	

Kurumların %56,3'nün tarayıcı sayısı 11 ile 100 arasında, %1,4'ünün 501 ile 800 arasında bulunmaktadır, %98,6'sının tarayıcısı 500 ve daha az sayıda olduğu görülmektedir.

Çizelge 9.22. Bilgisayar ve yan donanımları için izlenen bakım yöntemleri dağılımı (C-22)

Donanım bakımları nasıl yapılıyor	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
Kendi imkanlarıyla	45	35,7	55,6
Çağrı yöntemi ile	29	23,0	35,8
Yıllık parçalı bakım ile	38	30,2	46,9
Yıllık parçasız bakım ile	10	7,9	12,3
Diğer	4	3,2	4,9
Toplam	126	100,0	155,6

Kurumların gerçekleştirdiği bakım işlerinde en yüksek oranla kendi imkanlarını ve yıllık parçalı bakım yolunu benimsedikleri görülmektedir. Çağrı yöntemi de sık başvurulan yollardan birisidir.

Çizelge 9.23. BİM'lerin teknik destek verme durumuna göre dağılımı (C-23)

İş yeri desteği	Kurum sıklığı	%
Yeterli destek	59	72,8
Destek yok	6	7,4
Kısmen destek	16	19,8
Toplam	81	100,0

Kurumların çoğunda yöneticilerin BİM'ne teknik destek sağladığı görülmektedir.

9.3. Bilgi Güvenliği ve Fiziksel Güvenlik

Bilgi işlem merkezlerinin bilgi ve fiziksel güvenliğine ilişkin olarak sorulan D grubu sorulardan elde edilen cevapların sıklık dağılımları bu bölümde verilmiştir.

Çizelge 9.24. BİM'lerin güvenlik yazılımı kullanma durumuna göre dağılım (D-26)

Güvenlik yazılımı kullanımı	Kurum sıklığı	%
Kullanılıyor	81	98,8
Kullanılmıyor	1	1,2
Toplam	82	100,0

Düşük oranda da olsa halen güvenlik yazılımı kullanmayan kurumların olduğu görülmektedir.

Çizelge 9.25. BİM'lerin güvenlik için ayrılmış donanım kullanma durumuna göre dağılım (D-27)

Güvenlik için donanım kullanımı	Kurum sıklığı	%
Kullanan	76	95,0
Kullanmayan	4	5,0
Toplam	80	100,0

Kurum bilgi işlem merkezlerinin %98,8'i güvenlik yazılımına sahip olmakla birlikte, %95'i güvenlik yazılımı için donanım bulundurmaktadır.

Çizelge 9.26. BİM'lerin birden fazla antivirüs kullanma durumuna göre dağılım (D-29)

İkinci antivirüs kullanımı	Kurum sıklığı	%
Kullanan	32	39,5
Kullanmayan	49	60,5
Toplam	81	100,0

Kurum bilgi işlem merkezlerinin %39,5 i ikinci bir antivirüs kullanmayı tercih etmiş, sistemlerinde güvenlik açısından iki aşamalı filtre kullandıklarını ifade etmişlerdir. Antivirüs kullanım konusunda kurumlar yüksek seviyede hassasiyet göstermektedir. Tüm kurumların antivirüs kullandığı gözlenmiştir. İkinci antivirüs kullanılması durumunda güvenliğin daha yüksek seviyeye çıkacağı, virüs saldırılarının en az

seviyeye ineceği düşünülerek, kurumların %39'u ikinci antivirüs programı kullanmayı tercih etmişlerdir.

Çizelge 9.27. BİM'lerin antivirüs güncelleme yöntemlerine göre dağılımı (D30)

Yazılım güncelleme yöntemleri	Gözlemler	Gözlem %
Sistem merkezinden yapılmakta	71	87,7
Tek tek dolaşarak yüklenmekte	3	3,7
Sunucular üzerinden yüklenmekte	5	6,2
Diğer	2	2,5
Toplam	81	100,0

Kamu kurumlarındaki bilgi işlem merkezlerinin %87,7 si antivirüs yazılım güncellemelerini tek noktadan sistem merkezinden güncellemektedir. Bu durum kurum bilgi işlem merkezlerinin domain (alan) alt yapısına dahil olduğunu göstermektedir. Domain alt yapısı ise kurumun güvenlik alt yapısının daha güvenli bir ortamda bulunduğunun göstergesidir.

Çizelge 9.28. BİM'lerin kripto kullanım durumuna göre dağılım (D-31)

Güvenlik için kripto kullanımı	Gözlemler	%	Gözlem %
Kullanan	30	36,6	37,5
Kullanmayan	50	61,0	62,5
Toplam	80		100,0

Kamu kurum ve kuruluşlarında bilgi güvenliği ile ilgili önlemlerin alınmasında kripto kullanımının yaygın olmadığı, veri alış verişi yapan kurumların kripto kullandığı gözlenmiştir. Kurumların %37,5'i kripto (şifreleme) kullanmaktadır.

Çizelge 9.29. E-posta kullanımında alınan güvenlik önlemlerine ilişkin dağılım (D-32)

E-posta kullanımında alınan önlemler	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
E-posta şifreleri	17	11,0	21,0
Güvenlik yazılımları	64	41,3	79,0
Antivirüs yazılımı	72	46,5	88,9
Diğer	2	1,3	2,5
Toplam	155	100,0	191,4

E-posta kullanımı sırasında zarar görmemek için kurumların çok büyük bir kısmı antivirüs yazılımı ve yine onun kadar olmasa da büyük bir oranda güvenlik yazılımı kullanmayı tercih etmektedir. Kullanılan yöntemler arasında antivirüs yazılımı %46,5'luk bir oran oluşturmaktadır.

Çizelge 9.30. BİM'lerin Saldırı tespit sistemleri bulundurma durumuna göre dağılımı (D-33)

Saldırı tespit sisteminin varlığı	Gözlemler	Gözlem %
Var	51	63,8
Yok	29	36,3
Toplam	80	100,0

Kurumların önemli bir oranının saldırıyı önceden tespit edecek (IPS) sistemleri kullanmadığı görülmektedir.

Çizelge 9.31. BİM'lerin güvenlik politikasının varlığına göre dağılım (D-34)

Güvenlik politikası dokümanı	Gözlemler	Gözlem %
Var	41	51,3
Yok	39	48,8
Toplam	80	100,0

Kurumların çoğunda ISO 27001 standardına uyumlu güvenlik politikası bulunmamaktadır.

Çizelge 9.32. BİM'lerins Sakıncalı siteler için filtreleme durumuna göre dağılımı (D-35)

Sakıncalı sitelere filitreleniyormu	Gözlemler	%	Birikimli %
Evet yapılıyor	77	93.90	93.90
Hayır yapılmıyor	5	6.1	100.0
Toplam	82	100.0	

Az da olsa halen kurumların bir kısmının sakıncalı internet sitelerine filtre uygulamadıkları görülmektedir.

Çizelge 9.33. BİM'lerin yedekleme alma durumunu göre dağılım (D-36)

Sistem yedeklemesi	Gözlemler	%
Yedekleme yapılıyor	81	98,8
Yedekleme yapılmıyor	1	1,2
Toplam	82	100,0

Çizelge 9.34. BİM'lerin yedekleme sıklığına göre dağılım (D-37)

Yedekleme alma sıklığı	Gözlemler	%	Gözlemler %	Sıklık%
Her gün	67	81,7	82,7	82,7
Her hafta	8	9,8	9,9	92,6
Onbeş günde bir	2	2,4	2,5	95,1
Her ay	1	1,2	1,2	96,3
Diğer	3	3,7	3,7	100,0
Toplam	81		100,0	

Kamu kurum ve kuruluşlarındaki bilgi işlem merkezlerinin tamamına yakını sistemlerinde bulunan bilgilerin yedeklerini almaktadırlar. Kurumların %82,7'si her gün bilgilerinin yedeklerini alırken, %9,9'u her hafta yedekleme almaktadırlar.

Çizelge 9.35. BİM'lerin kişisel bilgilerin tutulması durumuna göre dağılım (D-38)

Kişisel bilgiler tutulması	Kurum sıklığı	%
Tutuluyor	43	52,4
Tutulmuyor	39	47,6
Toplam	82	100,0

Kurumların %52,4'ünün bilgi işlem merkezlerindeki veri tabanlarında kişisel bilgiler tutulmaktadır.

Çizelge 9.36. Kişisel bilgilerin güvenliğinin sağlanması ile ilgili dağılım (D-39)

Kişisel bilgi güvenliğinin sağlanma biçimi	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
Firewall (güvenlik duvarı) ile	36	32,7	83,7
Erişim şifrelerini sınırlandırarak	31	28,2	72,1
Verileri şifreleyerek	7	6,4	16,3
Sunuculara kontrollü erişim sağlayarak	33	30,0	76,7
Diğer	3	2,7	7,0
Toplam	110	100,0	255,8

Kurumlar yetkisiz kişilerin sisteme erişimini engellemek amacıyla çeşitli yöntemlere başvurmuşlardır. Kurumların %83,7'si güvenlik duvarını devreye sokarak bilgi güvenliğini sağlamaya çalışırken, yine %72,1 oranında da erişim şifrelerini sınırlandırarak kişisel bilgi güvenliğini sağlamaktadır. Verilerin şifrelenmesi en az kullanılan yöntemdir.

Çizelge 9.37. BİM'lerin saldırı tespiti ve izleme yapılması durumuna göre dağılımı (D-40)

Saldırı tespiti ve izleme yapılması	Kurum sıklığı	%
Yapılmakta	69	84,1
Yapılmamakta	13	15,9
Toplam	82	100,0

Kurumların büyük kısmı saldırı tespiti ve izleme yapmasına rağmen dikkate değer bir oranı da yapmamaktadır.

Çizelge 9.38. Kurumların saldırıda bulunulma durumuna göre dağılımı (D-41)

Sisteminize saldırı	Kurum sıklığı	%
Yapıldı	32	39
yapılmadı	50	61
Toplam	82	100,0

Kurumların oldukça yüksek bir oranda sistemlerine saldırı durumuyla karşılaştığı görülmektedir.

Çizelge 9.39. Saldırıya maruz kalan bilgi işlem merkezlerinin uğradığı zarar türlerinin dağılımı D-42

Saldırı sonucu sisteme verilen zararlar	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
Web sayfası çalışamaz duruma geldi	20	55,6	62,5
E-posta erişimi engellendi	6	16,7	18,8
Ağ erişimi engellendi	4	11,1	12,5
Verilerin içeriği değiştirildi	1	2,8	3,1
Herhangi bir zarar görmedi	5	13,9	15,6
Toplam	36	100,0	112,5

Saldırıya uğrayan kamu kurumları bilgi işlem merkezlerinin saldırı sonucu %15,6'sı her hangi bir zarara görmemiştir. Saldırıya uğrayan kurumların %62,5'nin web sitesinin çalışmaz duruma geldiği, %18,8'inin ise e-posta erişimlerinin engellendiği görülmektedir. Veri tabanlarına erişilerek bilgilerinin içeriği değiştirilen kurumların oranı ise %3,1'dir.

Çizelge 9.40. Saldırıya maruz kalan sistem merkezlerinin uğradığı zarar türlerine göre dağılımı (D-43)

Zarar türü	Kurum sıklığı	%
Maddi zarar gördü	5	16.67
Manevi zarar gördü	25	83.33
Toplam	30	100.00

Saldırıya uğrayan kurumların büyük bir kısmının maddi zarardan ziyade, prestij kaybı biçiminde manevi zarar gördükleri gözlenmektedir.

Çizelge 9.41. BİM'lerin güvenlik denetimi yapılma durumuna göre dağılımı (D-44)

Güvenlik denetimi	Kurum sıklığı	%
Yapılıyor	50	62,5
Yapılmıyor	30	37,5
Toplam	80	100,0

Kurumların önemli bir oranında, bilgi işlem merkezlerinin periyodik olarak güvenlik denetimi yapılmadığı görülmektedir.

Çizelge 9.42. BİM'lerin domain yapısına sahiplik bakımından dağılımı (D-45)

Domain yapısına sahiplik	Kurum sıklığı	%
Var	73	90.12
Yok	8	9.88
Toplam	81	100.00

Kurumlar network lerinde daha güvenli çalışabilmeleri için kendilerine özgü alan yapıları oluşturmaktadırlar. Kurumların %90,12'sinin iç ağlarında (domain) alan yapısı oluşturduğu gözlenirken, halen bir kısmının bu yapıya sahip olmadığı görülmektedir.

Çizelge 9.43. Kurumların arasında ağ bağlantısı durumuna göre dağılımı (D-46)

Kurumlar arası ağ bağlantısı	Kurum sıklığı	%
Var	51	62,2
Yok	31	37,8
Toplam	82	100,0

Kurumların %62,2'si bilgi alış verişini sağlamak amacıyla kendi aralarında protokol imzalamış, aralarında kapalı devre bağlantı oluşturmuşlardır. Bu bağlantılar Avrupa Birliği uyum yasaları çerçevesinde, e-devlet projelerinin uygulamalarında kullanılmaktadır.

Çizelge 9.44. Kurumların aralarındaki iki yönlü bilgi alış verişi durumuna göre dağılım (D-47)

İki yönlü ağ bağlantısı	Kurum sıklığı	%
Var	50	98.04
Yok	1	1.96
Toplam	51	100,0

Kurumlar sistemlerini e-devlet kapısı kapsamında bilgi akışını tek yönlü bilgi almak/vermek ya da çift yönlü bilgi alıp vermek için kurmuşlardır. Kurumlar arası ağ bağlantısı olan kurumların tamamına yakınının iki yönlü bağlantıya sahip oldukları görülmektedir.

Çizelge 9.45. Kurumların aktif dizin yapısına sahip olma durumuna göre dağılım (D-48)

Aktif dizin varlığı	Kurum sıklığı	%
Var	70	85,4
Yok	12	14,6
Toplam	82	100,0

Bilgi güvenliğinin önemli unsurlarından birisi olan aktif directory yapısına kurumların %85,4'ünün sahip olduğu görülmektedir.

Çizelge 9.46. Kurum çalışanlarının sisteme login olma durumuna göre dağılımı (D-50)

Sisteme login olma yöntemleri	Gözlemler	%
Kullanıcı şifreleri ile	79	96,3
Kart ve şifre ile	2	2,4
Diğer	1	1,2
Toplam	82	100,0

Kurumlarda sistemlere erişim imkanı çok büyük bir oranla, her kullanıcıya bir şifre verilerek gerçekleştirilmektedir.

Çizelge 9.47. Bilgi işlem çalışanlarının sistem odalarına giriş-çıkış yöntemlerine göre dağılımı (D-51)

Güvenlik için sistem odasına giriş çıkış	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
Kartlı sistemle	56	57,1%	69,1%
Parmak izi kullanarak	14	14,3%	17,3%
Tuş takımı üzerinden şifre girerek	11	11,2%	13,6%
Diğer	17	17,3%	21,0%
Toplam	98	100,0%	121,0%

Sistem odalarına giriş güvenliği kurumlarda büyük oranda kartlı sistemle sağlanmaktadır. Parmak izi ve diğer yöntemler de daha az oranda kullanılmaktadır.

Çizelge 9.48. Kurumların acil durum yönetimi için verilen yazılı talimat durumuna göre dağılım (D-52)

Sistem odası acil durum yazılı talimatı	Kurum sıklığı	%
Var	41	50,0
Yok	41	50,0
Toplam	82	100,0

Kurumlar bilgi işlem merkezlerinde bulunan sistem odaları için çeşitli güvenlik önlemleri alırken, acil durumlarda alacağı tedbirleri de düşünmelidir. Bunun için

kurumların %50'sinin acil durum yönetimi için yazılı talimatı bulunurken, diğer %50 sinin böyle bir önlemi bulunmamaktadır.

Çizelge 9.49. Kurumların bilgi işlem merkezine girişlerde kapı geçiş güvenliği durumuna ilişkin dağılım (D-54)

Kurum çalışanlarına BİM girişleri	Cevap sıklığı	%	Gözlem%
Herhangi bir güvenlik önlemi yok	50	76,9	56,3
Kurum kartı ile girişler yapılıyor	4	6	12,5
Özel giriş kartı alarak	3	4,6	9,4
İzine bağlı kimlik göstererek	2	3	6,3
Diğer	6	9,2	18,8
Toplam	65	100,0	103,1

Kurum personeline açık olan bilgi işlem merkezlerinin %56,3'ü hiçbir güvenlik önlemi alma ihtiyacı duymamaktadır. BİM merkezine girişler en yüksek oranda kurum giriş kartlarıyla sağlamaktadır. Bu durum güvenliğin bilgi işlem merkezleri açısından yetersiz olduğunu ortaya koymaktadır.

Çizelge 9.50. Kurumların sistem odası yangın güvenliği sistemine göre dağılım (D-55)

Sistem odası yangın söndürme sistemi	Kurum sıklığı	%
Var	67	82,72
Yok	14	17,28
Toplam	81	100,0

Kurumlar güvenliklerini düşünürken olası tüm riskleri düşünmek zorundadır. Yangın söndürme sistemleri de bu güvenlik önlemlerinden birisi olmakla birlikte, kurumların dikkate değer bir oranı yangın söndürme sistemlerinin bulunmadığını belirtmiştir.

Çizelge 9.51. Kurumların kamera güvenliği sistemine göre dağılım (D-56)

Bina güvenlik kamera sistemi	Kurum sıklığı	%
Var	73	90,12
Yok	8	9,88
Toplam	81	100

Kurumların büyük bir kısmının kameralı güvenlik sistemleri mevcuttur.

Çizelge 9.52. Kurumların yazılı güvenlik standardına göre dağılım (D-57)

Yazılı güvenlik standardı	Kurum sıklığı	%
Yazılı güvenlik standardı var	46	56,1
Yazılı güvenlik standardı yok	36	43,9
Toplam	82	100,0

Kurumların %56,1'inin yazılı güvenlik standardının olduğu, %43,9'unda yazılı güvenlik standardının bulunmadığı görülmektedir.

Çizelge 9.53. Kurumların sistem yedeğinin başka bir bölgede (disaster recovery) saklanması durumuna göre dağılımı (D-58)

Sistemlerin Yedeği (disaster)	Kurum sıklığı	%
Var	18	22,0
Yok	64	78,0
Toplam	82	100,0

Sistem odalarının fiziksel olarak yedeklenmesi, sistemlerin kesintiye uğramaması açısından önem arz etmektedir. Felaket durumlarında, bilgi akışının kesilmemesi, hizmetlerin sürekliliği, devlet işlerinin devamlılığı bakımından benzer bir yedeğini başka bir bölgede kurması gerekliliği oluşmaktadır. Kurum bilgi işlem merkezlerinin %78'inin sistem odalarının yedeği (disaster recovery) başka bir coğrafi bölgede bulunmamaktadır.

Çizelge 9.54. BİM'lerine ait yazılı felaket senaryosunun varlığına göre dağılımı (D-59)

Yazılı felaket senaryosu	Kurum sıklığı	%
Var	18	22,0
Yok	64	78,0
Toplam	82	100,0

Bilgi işlem merkezlerinin felaket sonrası sistemlerin çökmesi, cihazların zarar görmesi durumunda, görevlendirilecek personelin belirlenmesi, yerine konacak cihazların yedeğinin bulundurulması her durumun yazılı olarak bulundurulması gerekmektedir. Kurumların %78 gibi büyük bir oranının böyle bir yazılı felaket senaryosu olmadığı görülmektedir.

Çizelge 9.55. Personelin yetkilendirilmesi ile ilgili dağılım (D-60)

Kullanıcıların bilgisayar üzerindeki yetkisi	Cevap sıklığı	Cevaplara %	Kurumlara göre %
Herhangi bir sınırlandırma yok	14	9,0	17,3
Sadece kendi işi ile sınırlandırılmış	36	23,1	44,4
Görev yetki çerçevesinde sınırlandırılmış	53	34,0	65,4
Sohbet ve haberleşmeler yasaklanmış	25	16,0	30,9
İnternet çıkışları sınırlandırılmış	28	17,9	34,6
Toplam	156	100,0	192,6

Kamu kurumlarının %83'ü bilgisayarlar üzerinde kullanıcılara çeşitli sınırlama getirmiştir. Getirilen sınırlamalar içinde en yüksek oranı "görev yetki çerçevesinde sınırlandırma" oluşturmaktadır. Kurumların önemli bir oranında da diğer sınırlandırma türleri uygulanmaktadır. Bununla beraber, herhangi bir sınırlandırma getirmeyen kurum oranı da dikkat çekicidir.

9.4. Yazılım ve E-imza Güvenliği

Çalışmanın bu kısmında kurumlarda kullanılan yazılımlar ve e-imza uygulamalarına ilişkin bulgular yer almaktadır.

Çizelge 9.56. Kurumları kullanıcı desteğinin verilme durumuna göre dağılımı (E-61)

Kullanıcılara destek	Kurum sıklığı	%
Veriliyor	79	96,34
Verilmiyor	3	3,66
Toplam	82	100,00

Kurum bilgi işlem merkezlerinin görevlerinden biri de, kurumda çalışan diğer birimlerdeki kullanıcılara da destek vermektir. Kurumların çoğunda bilgi işlem merkezlerinin diğer birimlerde çalışan personel bilgisayarlarına destek verdiği

Çizelge 9.57. Kurumların açık kaynak kodu kullanım durumuna göre dağılımı (E-62)

Açık kaynak kodu	Kurum sıklığı	%
Kullanılıyor	79	96,3
Kullanılmıyor	3	3,7
Toplam	82	100,0

Çizelge 9.58. Yanıtların açık kaynak kodlu yazılım türlerine göre dağılımı (E-63)

Açık kaynak kodu türü	Cevap sıklığı	Cevaplara göre %	Kurumlara göre %
Linux	47	54,0	85,5
Pardus	7	8,0	12,7
Open Office	23	26,4	41,8
Diğer	10	11,5	18,2
Toplam	87	100,0	158,2

Kurumların %96,3 gibi büyük bölümünde açık kaynak kodu yazılımları kullanılmaktadır. Bu durum yazılım sektörünün açık kaynak kodlu yazılımlara yönlendiğini göstermektedir. Maliyeti yüksek olan Windows yerine kurumlar daha çok Linux işletim sistemini tercih etmektedirler. Açık kaynak kodlu yazılımların içinde en ağırlıklı kullanılan yazılım %54 ile Linux olarak görülmektedir. Microsoft ofis işletim sistemi yerini ise ücretsiz olan open ofis almaya başlamıştır. Open ofis'in açık kaynak kodlu yazılımdaki yüzdesi ise %26,4'tür.

Çizelge 9.59. Kurumların ofis otomasyonu kullanım durumuna göre dağılımı (E-64)

Ofis yazılımları kullanımı	Kurum sıklığı	%
Kullanılıyor	51	62,20
Kullanılmıyor	31	37,80
Toplam	82	100,00

Kurumların %62,20'si ofis otomasyonu kullanarak işlerini yürütürken, %37,80'i kurumlarında başka yazılımlar kullanmaktadırlar.

Çizelge 9.60. Kurumların e-devlet uygulamalarının varlığına ilişkin dağılım (E-65)

e-devlet uygulaması	Kurum sıklığı	%
Var	47	57,3
Yok	35	42,7
Toplam	82	100,0

Kamu kurumlarında e-devlet uygulamalarına yönelik çalışmalar son zamanlarda öncelikli projeler arasına girmiştir. Kurumlar Avrupa Birliği uyum yasaları çerçevesinde bu projelere ağırlık vermiştir. Kurumların %57,3'ünde vatandaşla ilgili e-devlet uygulamaları bulunmaktadır.

Çizelge 9.61. Kurumların e-imza kullanım durumuna göre dağılımı. (E-66)

E-imza kullanımı	Sıklık	%
Kullanılıyor	22	26,8
Kullanılmıyor	60	73,2
Toplam	82	100,0

5070 sayılı E-imza yasasının Ocak 2004 yılında yürürlüğe girmiş olmasına rağmen kurumlar elektronik imza konusunda fazla yol kat edememişlerdir. Kurumların ancak %26,8'i elektronik imzayı kullanmaktadır, %73,2'si henüz kullanım aşamasına gelmemiştir.

Çizelge 9.62. Kurumların e-imza kullanım alanlarına göre dağılım (E-68)

E-imza kullanım alanları	Kurum sıklığı	%
Sadece kurum içinde	12	54,55
Sadece kurum dışında	7	31,82
Kurum içi ve kurum dışında	3	13,64
Toplam	22	100,00

Kurumların yarıdan fazla kısmı e-imzayı sadece kurum içinde kullanmaktadır.Her iki alanda da e-imza kullananların oranı ise %13,64 tür.

Çizelge 9.63. Kurumların e-imza desteği alma durumuna göre dağılımı (E-69)

E-imza desteği alma	Sıklık	%
Destek alan	12	54,55
Destek almayan	10	45,45
Toplam	22	100.00

Kurumlar e-imza konusunda %54,55'i dışarıdan destek almak suretiyle elektronik imza çalışmalarını sürdürmüştür.

9.5. BİM Yöneticilerinin Genel Algılamaları

Soruların bu son kısmında ise BİM yöneticilerin genel algılamalarına ilişkin görüşlerine ilişkin analizler gerçekleştirilmiştir.

Çizelge 9.64. Üst düzey yöneticilerin teknolojiye bakış açısına göre dağılımı (F-70)

Kurum üst yönetiminin teknolojiye bakışı	Kurum sıklığı	%
Eski teknolojileri tercih ediyor.	1	1,2
Yeterli desteği veriyor	47	57,3
Destek veriyor fakat yeterli değil	34	41,5
Toplam	82	100,0

Kamu kurumlarında karar verici düzeydeki yöneticiler teknolojiye uzak olmaları durumunda, bilgi işlem merkezlerine yeterli desteği vermekte zayıf kalmaktadır. Kurum üst yönetimlerinin önemli bir kısmının desteğinin yetersiz olduğu görülmektedir.

Çizelge 9.65. Kurumların sunuculardaki bilgilerin güvenlik durumuna göre dağılımı (F-71)

Sunucularda tutulan bilgiler güvenliği	Kurum sıklığı	%
Güvenli	70	85,4
Güvenli değil	12	14,6
Toplam	82	100,0

Kurum bilgi işlem yöneticilerinin %85,4'ü sunucular üzerindeki bilgilerin güvenli olduğunu ve yeterli düzeyde güvenlik önlemlerinin alındığını ifade ederken, önemli sayılabilecek bir oranının ise bilgi güvenliğini yeterli görmediği görülmektedir.

Çizelge 9.66. Kurumların bilgi işlem çalışanlarının hukuki sorumluluklarını bilme durumuna göre dağılımı (F-72)

Hukuki sorumluluklarını bilme	Sıklık	%
Biliyor	74	90,24
Bilmiyor	8	9,76
Toplam	82	100

BİM yöneticilerinin büyük kısmı yasal sorumluluklarından haberdar olduğunu belirtmiştir.

Çizelge 9.67. BİM çalışanlarının memnuniyet durumuna göre dağılımı (F-73)

Çalışma ortamından memnuniyet	Sıklık	%
Memnun	76	92,7
Memnun değil	6	7,3
Toplam	82	100,0

Kurum BİM yöneticilerinin %92,7'si bilgi işlem biriminde çalışmaktan mutlu olduklarını ifade etmişlerdir.

Çizelge 9.68. Kurum çalışanların aldığı maaş memnuniyet durumuna göre dağılımı (F-74)

Aldığınız maaştan memnun musunuz	Sıklık	%
Memnun	15	18,3
Memnun değil	67	81,7
Toplam	82	100,0

BİM yöneticileri çalıştıkları birimden yüksek bir oranla memnun olduklarını belirtirken, yine yüksek bir oranda maaşlarından memnun olmadıklarını belirtmişlerdir.

9.6. Değişkenler Arası İki Yönlü İlişki Analizleri

Çalışmanın bu kısmında BİM'lerine ilişkin bazı değişken çiftleri arasında yapılan ilişki analizleriyle ilgili bulgular yer almaktadır. Araştırmanın örneklemi tesadüfi olarak seçilmediğinden ki-kare istatistiğine dayalı bu ilişki analizlerine ihtiyatla yaklaşmak gerekir. Örneklemde tesadüfilik sağlanmamasına rağmen, yapılan bu analizler yine de yığın hakkında bir öngörüde bulunmaya yardımcı olabilir.

Çizelge 9.69. BİM'lerin idari yapılanma türü ile bilgi işlem eğitim.sıklığına göre dağılımı (A-1, A-6)

İdari birimler		Eğitim				Toplam
		Sıklıkla	Arasıra	Nadiren	Diğer	
BİM Genel Md.	Sıklık	0	1	0	1	2
	%	,0	50,0	,0	50,0	100,0
BİM Başkanlığı	Sıklık	0	1	0	0	1
	%	,0	100,0	,0	,0	100,0
BİM Daire Bşk	Sıklık	2	11	11	3	27
	%	7,4	40,7	40,7	11,1	100,0
BİM Müdürlüğü	Sıklık	4	10	8	1	23
	%	17,4	43,5	34,8	4,3	100,0
Toplam	Sıklık	6	23	19	5	53
	%	11,3	43,4	35,8	9,4	100,0

Bilgi işlem faaliyetleri Genel Müdürlük altında yürütülen kurumların %50'si arasıra eğitim verirken, daire başkanlığı olarak faaliyetini sürdüren kurumların %40,7'sinde arasıra eğitim verilmektedir. Bununla beraber, $\chi^2 = 7{,}813$ olarak hesaplanmış olup, $p = 0{,}531 > 0{,}05$ olduğundan idari yapı ile aldıklar ı eğitim sıklığı arasında anlamlı bir ilişki bulunmamaktadır.

Çizelge 9.70. BİM'lerin idari yapı ve kullanıcı sayısına göre dağılımı (A-1, A-2)

İdari birimler		Kullanıcı sayısı				Toplam
		50-100	100-500	500-1000	1000+	
BİM Genel Md.	Sıklık	0	0	0	2	2
	%	,0	,0	,0	100	100
BİM Başkanlığı	Sıklık	0	0	0	3	3
	%	,0	,0	,0	100	100
BİM Daire Bşk	Sıklık	0	7	7	20	34
	%	,0	20,6	20,6	58,8	100
BİM Müdürlüğü	Sıklık	4	18	7	14	43
	%	9,3	41,9	16,3	32,6	100
Toplam	Sıklık	4	25	14	39	82
	%	4,9	30,5	17,1	47,6	100

Bilgi işlem faaliyetlerini bilgi işlem müdürlüğü ve daha alt seviyede yürüten kamu kurumlarının %41,9'unun kullanıcı sayısı 100-500 aralığındadır. Daire başkanlığı olarak faaliyetini yürüten kamu kurumlarının %58,8'inin kullanıcı sayısı 1000'in üzerindedir. Hücrelerin %82,5'inde beklenen frekanslar 5 den daha az olduğundan Fisher'in Exact testi ile yapılan analizde $p = 0,069 < 0,10$ olduğundan $\alpha = 0,10$ düzeyinde anlamlı ilişki olduğu söylenebilir.

Çizelge 9.71. BİM'lerin güvenlik standardı varlığı ve sistem yedeği durumuna göre dağılımı (D-57,D-58)

Yazılı güvenlik standardı		Sistemin yedeği (disaster recovery)		Toplam
		Var	Yok	
Var	Sıklık	17	29	46
	%	37,0	63,0	100,0
Yok	Sıklık	1	35	36
	%	2,8	97,2	100,0
Toplam	Sıklık	18	64	82
	%	22,0	78,0	100,0

Yazılı güvenlik standardı olan kurumların %37'sinin bir bölgede sistemlerinin yedeği (disaster recovery) bulunmaktadır. Yazılı güvenlik standardı olmayan kurumlardan %97,2'sinde sistemlerinin yedeği (disaster recovery) bir başka coğrafi bölgede yoktur.

Pearson'un $\chi^2 = 13,770$ olarak hesaplanmış olup, $p = 0,00 < 0,05$ olduğundan yazılı standardın varlığı ile kurumların başka bir coğrafi bölgede sistemlerin yedeğinin bulunması arasında istatistiksel olarak 0.05 düzeyinde anlamlı bir ilişki bulunmaktadır.

Çizelge 9.72. BİM'lerin güvenlik yazılımı kullanımı ve güvenlik donanımı kullanımına göre dağılımı. (D-26,D-27)

Güvenlik yazılımı kullanma		Güvenlik donanımı kullanma		Toplam
		Var	Yok	
Var	Sıklık	76	3	79
	%	96,2	3,8	100,0
Yok	Sıklık	0	1	1
	%	,0	100,0	100,0
Toplam	Sıklık	76	4	80
	%	95,0	5,0	100,0

Güvenlik yazılımı kullanan kurumların %96,2'sinde yazılımı üzerine yükleyebileceği ve güvenlik için ayırdığı donanımları bulunmaktadır. Eğer kurum güvenlik yazılımı kullanmıyor ise donanım alma ihtiyacı da duymamıştır.

Pearson'un χ^2 değeri 19,241 olup $p = 0,00 < 0,05$ olduğundan, güvenlik yazılımı ile güvenlik donanımı kullanımı arasında anlamlı bir ilişki bulunmaktadır.

Çizelge 9.73. BİM'lerin saldırı tespit sistemi ve yedekleme alma sıklığına göre dağılımı (D-33,D-36)

Saldırı tespit sistemleri		Yedekleme alma sıklığı				Toplam
		Her gün	Her hafta	Onbeş günde	Her ay	
Var	Sıklık	41	6	0	3	50
	%	82,0	12,0	,0	6,0	100,0
Yok	Sıklık	25	2	2	0	29
	%	86,2	6,9	6,9	,0	100,0
Toplam	Sıklık	66	8	2	3	79
	%	83,5	10,1	2,5	3,8	100,0

Saldırı tespit sistemi bulunan kurumların bilgi işlem merkezlerinin %82'sinde her gün yedekleme alınmaktadır. Saldırı tespit sistemleri bulunmayan kurumların bilgi işlem merkezlerinin %86;2'sinde günlük yedekleme yapılmaktadır.

Pearson'un $\chi^2 = 5,699\,\chi^2$ ve p = 0,127 > 0,05 olduğundan, yedekleme sıklığı ile saldırı tespit sisteminin varlığı birbirinden 0.05 anlamlılık düzeyinde bağımsızdır.

Çizelge 9.74. BİM'lerin saldırı tespit izleme sisteminin varlığı ve sistemlerin saldırıyla karşılaşma durumuna göre dağılımı.(D-40,D-41)

Saldırı tespit izleme		Saldırıda bulunma		Toplam
		Var	Yok	
Var	Sıklık	30	39	69
	%	43,5	56,5	100,0
Yok	Sıklık	2	11	13
	%	15,4	84,6%	100,0
Toplam	Sıklık	32	50	82
	%	39,0	61,0	100,0

Saldırı tespiti ve izleme yazılımı olan kurumların %43,5'ine saldırıda bulunulmuştur. Saldırı tespit ve saldırı izleme yazılımı olmayan kurumların ise %84,6'sına saldırıda bulunulmamıştır.

Pearson'un $\chi^2 = 3,628$ ve p = 0,057 > 0,05 olduğundan 0,05 düzeyinde anlamlı ilişki olduğu söylenemezken 0.10 düzeyinde anlamlı ilişkinin varlığından bahsedilebilir.

Çizelge 9.75. BİM'lerin sistemin yedeğinin alınması ile yazılı felaket senaryosu varlığına göre dağılımı.(D-58,D-59)

Sistemin yedeği başka bölgede		Yazılı felaket senaryosu		Toplam
		Var	Yok	
Var	Sıklık	8	10	18
	%	44,4	55,6	100,0
Yok	Sıklık	10	54	64
	%	15,6	84,4	100,0
Toplam	Sıklık	18	64	82
	%	22,0	78,0	100,0

Sistem yedeği (disaster recovery) başka bölgede olan kurumların %44'4'ünde yazılı felaket senaryosu bulunmaktadır. Sistemlerinin yedeği başka bölgede bulunmayan kurumların %84,4'ünde yazılı felaket senaryosu bulunmamaktadır.

Pearson'un $\chi^2 = 6,811$ olup, p = 0,00 < 0,05 olduğundan sistemlerinin yedeğinin bir başka bölgede olması ile kurumlarda yazılı bir felaket senaryosu bulunması arasında anlamlı bir ilişki bulunmaktadır.

Çizelge 9.76. BİM'de çalışanların iş yerinden memnuniyeti ve maaş memnuniyetine göre dağılımı (F-73,F-74)

BİM çalışma memnuniyeti		Çalışanlarında maaş memnuniyeti		Toplam
		Var	Yok	
Memnun	Sıklık	15	61	76
	%	19,7	80,3	100,0
Memnun değil	Sıklık	0	6	6
	%	,0	100,0	100,0
Toplam	Sıklık	15	67	82
	%	18,3	81,7	100,0

Bilgi işlem merkezlerinde çalışmaktan memnun olan teknik personelin %80,3'ü aldıkları maaştan memnun olmamaktadır. Çalıştıkları yerden memnun olmayan personel aynı zamanda aldıkları maaştan da memnun değiller.

Pearson'un $\chi^2 = 1,449$ ve p = 0,229 > 0,05 olduğundan, BİM çalışanlarının çalıştıkları birimden memnuniyetleri ile, aldıkları maaş memnuniyeti arasında anlamlı bir ilişki bulunmamaktadır.

9.7. Çeşitli Kategoriler Bakımından Kurumsal Benzerlikler-Kümeleme Analizleri

Bu kısımda değişkenlerin ana kategorileri bakımından benzerliklerine göre kurumların kümelenmesine ilişkin analiz bulguları verilmektedir.

9.7.1. Eğitim değişkenleri ne göre kümelenme (A6-A7)

Kamu kurumları BİM'inde çalışan personellerin "bilgisayar ve bilgisayar güvenliğini içeren eğitimleri alma sıklıkları ve hangi sıklıkta aldığına ilişkin değişkenlere göre kümeleme analizi gerçekleştirilmiştir. Eğitim türü çoklu seçmeli soru olduğundan her bir seçenek bir değişken olarak analize girmiş olup, kümeleme böylece toplam 7 değişken üzerinden yapılmıştır. Kurum BİM'leri eğitim değişkenlerine göre optimal 4 kümede toplanmıştır. Kümeleme kalitesi (Şekil.9.1. en soldaki şekil) iyiye yakın biçimde gerçekleşmiştir.

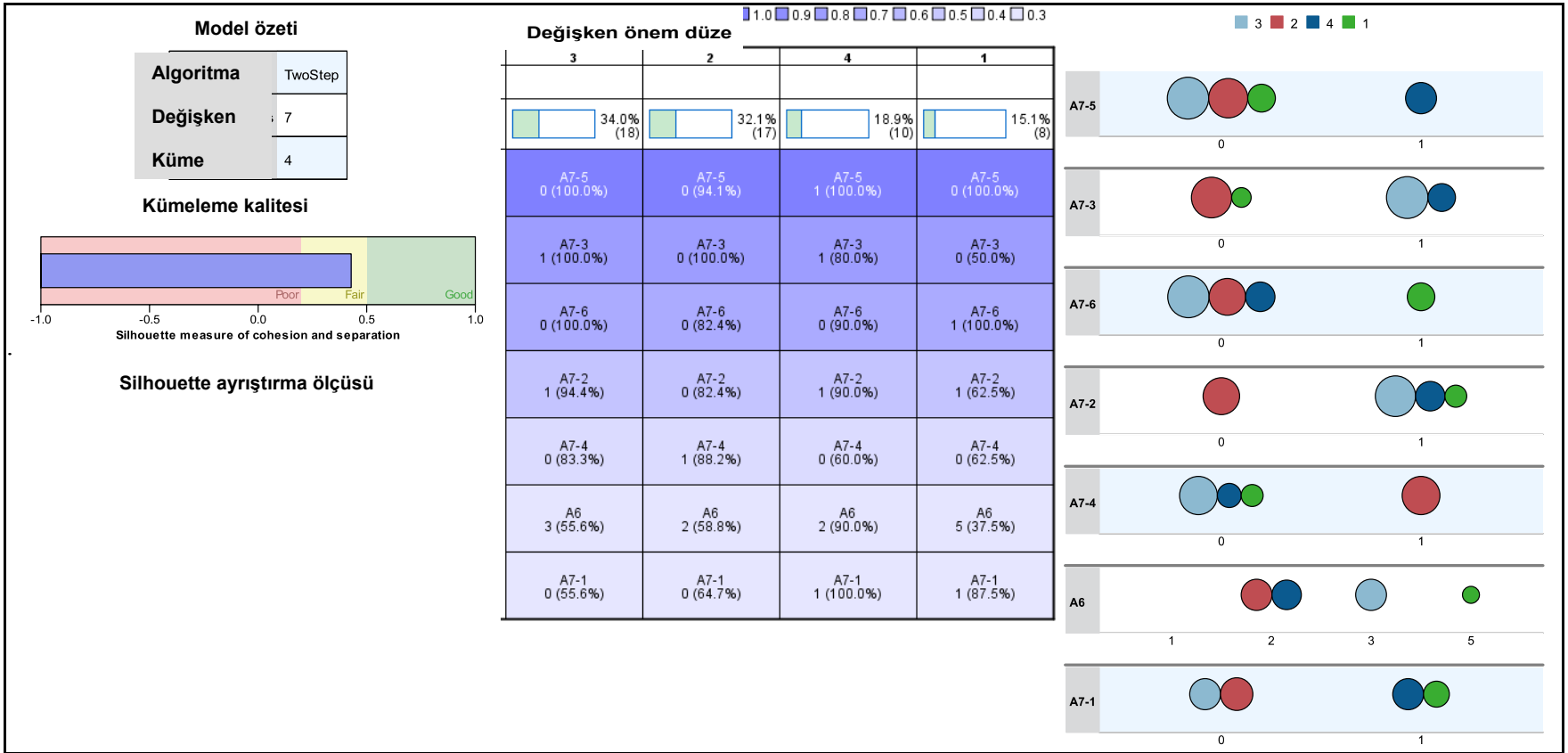
Kurumların %34'ü üçüncü kümede yer alırken %32,1'i ikinci kümede, %18,9'u dördüncü kümede, %15,1'i ise birinci kümede yer almıştır. Kümeleme üzerindeki etki dereceleri bakımından değişkenler en önemliden önemsize doğru sıralanmıştır Değişkenlerin kümelenmesi sonucunda yedi değişken en çok benzerlik gösteren değişkenden, en az benzerlik gösteren değişkene doğru sıralanmıştır (ortadaki şekil). Kümeleme üzerine en büyük etkiyi "teknisyenlik eğitimi" değişkeni yapmışken, en az etkiyi de "PC güvenliği" değişkeni göstermiştir.

Şeklin en sağında ise değişkenler itibariyle kümelerin birbirine yakınlıkları görülmektedir. Bu kümelerde yer alan kurumların hepsinde de "teknisyenlik eğitimi" alınamaması yönünde yoğunlaşma vardır. Ofis programları kullanımı eğitimi değişkeni bakımından ikinci ve birinci kümede yer alan kurumlar birbirine benzerlik gösterirken çoğunlukla ofis programları kullanmayan kurumlar burada kümelenmiştir. İleri düzey kullanıcı eğitimi değişkeni bakımından üçüncü, dördüncü ve birinci küme içinde yer alan kurumlar birbirine benzerlik gösteren, ileri düzey kullanıcı eğitimi almayan kurumlar burada kümelenmiştir. Bilgisayar temel eğitimi bakımından üç, dört ve birinci kümeler birbirine benzerlik gösterirken, bilgisayar temel eğitimi alan kurumlar bu kümelerde toplanmıştır. Verilen eğitimlerin sıklığı bakımından iki ve dördüncü kümelerde yer alan kurumlar birbirine benzerlik göstermektedirler. Bu kümelerde bulunan kurumların çoğu eğitim sıklığı arasıra verilen kurumlardır. Üçüncü ve birinci kümelere giren kurumlar ise bunlardan

ayrılmaktadır. Üçüncü kümeye giren kurumların çoğu nadiren eğitim alırken, birinci kümede olan kurumlar diğer sıklıklarla eğitim almaktadır.

Şekillerin alt kısmında kümeler ve kümelere giren gözlemler verilmiştir. Gözlemler numaralarla ifade edilmiş olup, her bir numara bir kurumu tanımlamaktadır. Verilerin gizliliği nedeniyle numaraların hangi kurumları temsil ettiği burada tanımlanmamıştır.

Birinci küme genelde taşra teşkilatı olan kurumları kapsarken, üçüncü küme daha çok bakanlık yapısında olan kurumları kapsamaktadır.



Küme 3	Küme 2	Küme 4	Küme 1
2 6 9 10 12 16 29 42 44 45 46 50 53 58 63 65 68 74	1 13 14 17 28 39 43 47 49 54 55 69 72 75 78 79 80	7 8 38 32 40 51 59 61 62 71	11 20 24 35 66 70 73 77

Şekil9.1.Eğitimdeğişkenlerine göre kümeleme

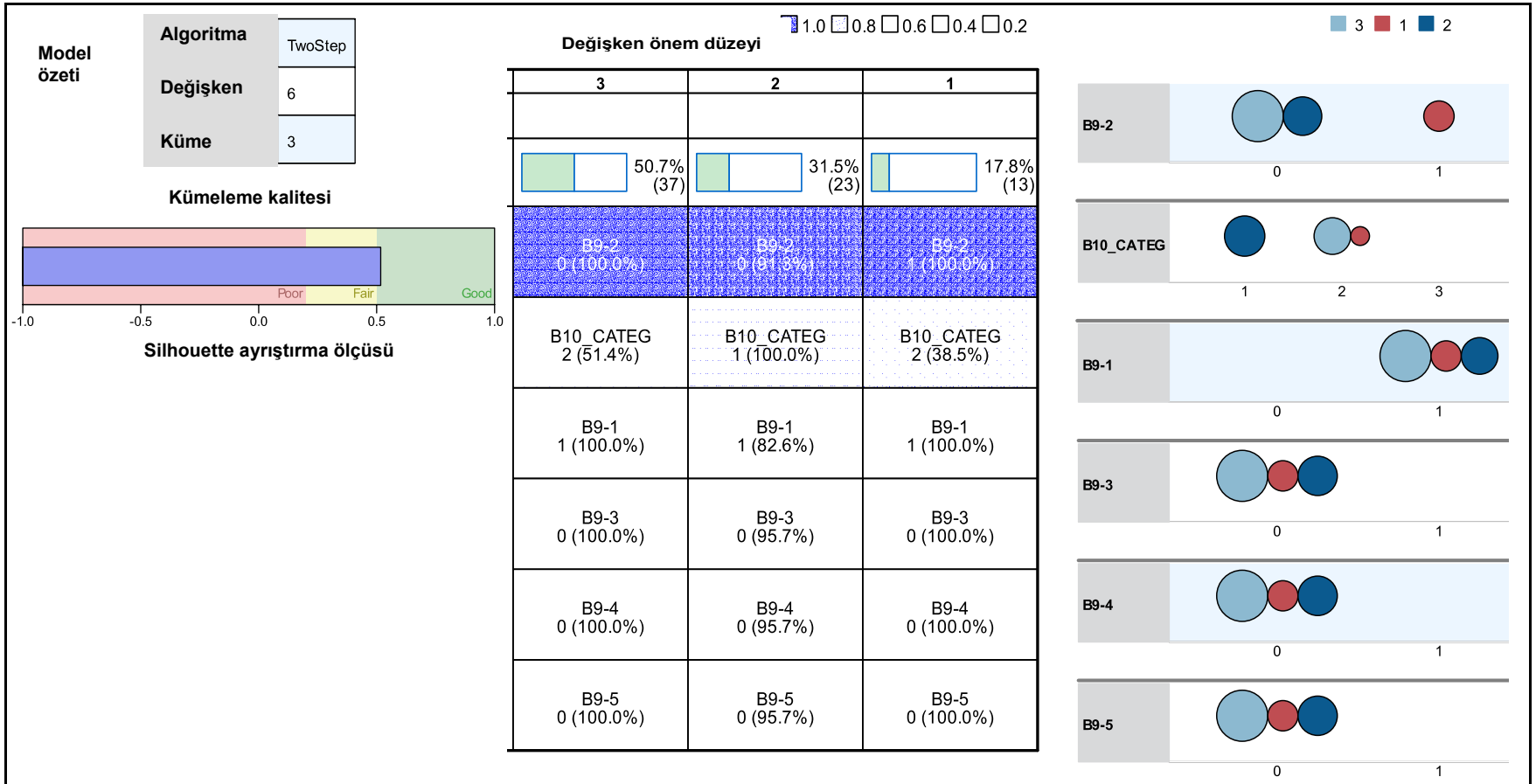
9.7.2. İnternet bağlantısı ve fiziksel alt yapısına göre kümeleme

Kurumlar ne tür İnternet bağlantısı kullandıkları ve internet hızı bakımından kümeleme analizine tabii tutulmuş, 6 değişken kullanılmıştır. Benzerlik göstermeleri bakımından 3 grupta kümeleme gerçekleşmiştir.

İnternet bağlantısı ile kurumlardaki internet hızları bakımından kümeleme kalitesi iyi bir düzeyde gerçekleşmiştir. Gerçekleşen 3 küme incelendiğinde Kurumların %50,7'si üçüncü kümede yer alırken, %31,5'i ikinci kümede, %17,8'i birinci kümede yer aldı. Kümeleme üzerindeki etki dereceleri bakımından değişkenler en önemliden önemsize doğru sıralanmıştır. Bu sıralamada kurumların internet bağlantı türlerinden ADSL bağlantı türünün en belirgin kümelemeye sahip değişken olduğu görüldü. Çoğunlukla bağlantı türünü ADSL olarak kullanmayan kurumlar burada kümelendi. Kurumları internet çıkış hızı değişkeni bakımından birbirine benzeyen kümeler sıralamasında ikinci önemli değişkeni oluştururken, internet çıkışlarını Metro ethernet olarak kullanan kurumlar üçüncü önem sırasında kümelenmiştir.

ADSL bağlantı türü bakımından üçüncü ve ikinci kümeler birbirine benzerlik gösterirken çoğunlukla ADSL bağlantı türünü kullanmayan kurumlar burada kümelenmiştir. İnternet hızı kullanımı bakımından üçüncü ve birinci kümelerdeki kurumlar birbirine benzerlik gösterirken, ikinci kümedeki kurumlar bunlardan ayrılmaktadır. Kurumların metro ethernet bağlantı türü bakımından incelendiğinde burada oluşan kümelerin tamamı birbirine benzerlik göstermektedir. Ve çoğunlukla bağlantı türünü Metro ethernet olarak kullanmaktadırlar. Diğer bağlantı türü olan değişkenlerin kümelenmesine bakıldığında ISDN, Dial-Up, X25 gibi bağlantı türleri her üç kümeyi oluşturan kurumlar arasında benzerlik göstermekte ve bu kurumlar çoğunlukla bu bağlantı türlerini kullanmamaktadır.

Kurumlar çoğunlukla bağlantı türlerini Metro ethernet olarak tercih etmektedirler. Üçüncü kümede çoğunlukla bakanlık ve genel müdürlük biçiminde olan kurumlar yer almaktadır.



Küme 3	Küme 1	Küme 2
1 6 7 8 11 13 14 15 16 19 20 21 24 25 38 28 30 33 35 36 39 40 45 52 54 57 58 59 66 68 69 71 72 7374 75 79	2 4 5 27 37 44 48 51 55 62 77 78 81	9 17 18 22 23 29 32 34 41 42 43 44 45 51 55 57 58 59 68 69 73 76 77 78 79 81

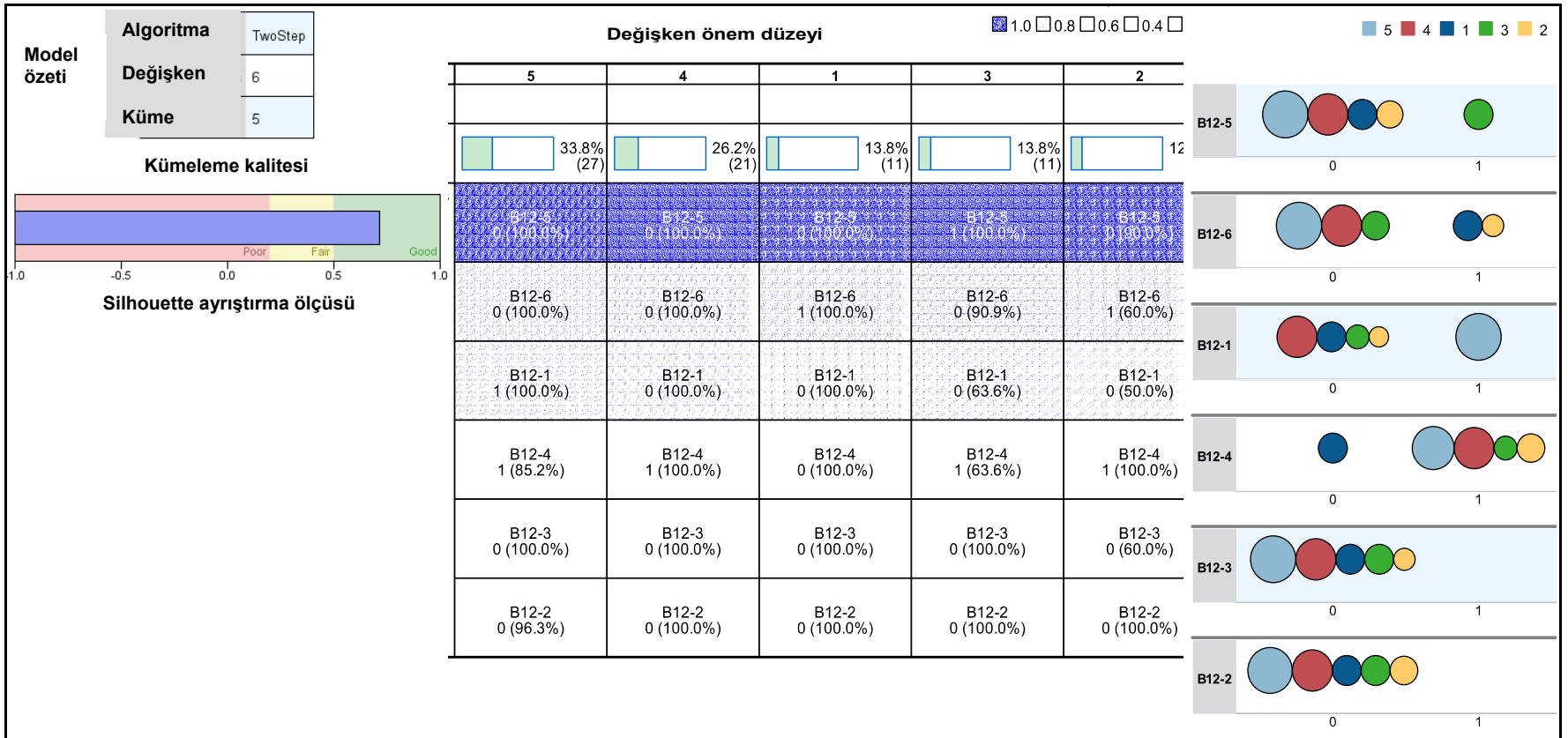
Şekil 9.2. İnternet Bağlantısı fiziksel altyapısına göre Kümeleme

9.7.3. İnternet kullanıcılarından gelen sorunlara göre kümeleme

Kurumlarda internet kullanımı bakımından kurumlar benzerlik açısından kümelenmiştir. Kurumlardaki internet sorunlarıyla ilgili 6 değişken kullanılmıştır. Benzerlik göstermeleri bakımından 5 grupta kümeleme gerçekleşmiştir.

İnternet kullanıcıları için Kümeleme kalitesi iyi biçimde gerçekleşmiştir. Kurumların %33,8'i beşinci ve %26,2'si dördüncü, kümede yer aldı. Değişkenler kümelenirken altı değişken en çok benzerlik gösteren değişkenden en az benzerlik gösteren değişkene doğru sıralandı. Bu sıralamada kümelerin oluşumunda diğer seçeneği diğer değişkenler içerisinde en önemli değişkeni içerdiği görüldü. Değişkenler önem sırasından azalan sırayla, internet kullanımında herhangi bir sorun yaşama, virüs saldırılarının bilgi kaybına neden olduğu, istenmeyen posta mesajlarının geldiği, kişisel bilgilerin elde edildiği ve kredi kartı kullanımında zarar gördüğü şeklinde sıralandı.

Diğer seçeneği bakımından beşinci, dördüncü, birinci ve ikinci kümeler birbirine benzerlik gösterirken, çoğu diğer seçeneğini cevaplamayan kurumlar burada yoğunlaşmıştır. "Herhangi bir sorun yaşamadım" değişkeni bakımından beşinci, dördüncü ve üçüncü kümede yer alan kurumlar birbirine benzerlik gösterirken çoğunlukla herhangi bir sorun yaşamayan kurumlar burada kümelenmiştir. Virüsten zarar gören ve bilgilerin kayıp olması değişkeni bakımından dördüncü, birinci, üçüncü ve ikinci kümeler içinde yer alan kurumlar birbirine benzerlik gösterirken, virüsten zarar görmeyen ve bilgi kaybı olmayan kurumlar burada kümelenmiştir. İstenmeyen ileti alma değişkeni bakımından beşinci, dördüncü, üçüncü ve ikinci kümeler birbirine benzerlik gösterirken çoğunlukla istenmeyen ileti almayan kurumlar bu kümelerde toplanmıştır. Kişisel bilgilerin başkalarının eline geçti değişkeni ve Kredi kartı kullanımından zarar görme değişkeni bakımından tüm kurumlar birbirlerine benzerlik göstermektedir. Bakanlık ve genel müdürlükler beşinci kümede yer alırken, yargılama faaliyeti gösteren kurumlar ve belediyeler çoğunlukla dördüncü kümede yer almışlardır.



Küme 5	Küme 4	Küme 1	Küme 3	Küme 2
3 4 5 6 7 8 11 12 14 15 16 17 21 22 38 27 30 32 40 45 54 55 56 58 63 74 76	10 13 19 24 34 36 41 43 46 47 48 49 53 57 61 64 68 69 71 72 78	1 37 39 42 50 51 52 59 67 8081	2 9 18 20 25 28 35 60 62 73 75	23 29 31 33 44 65 66 70 77 79

Şekil 9.3. İnternet Kullanıcı Sorunları Değişkenine Göre Kümeleme

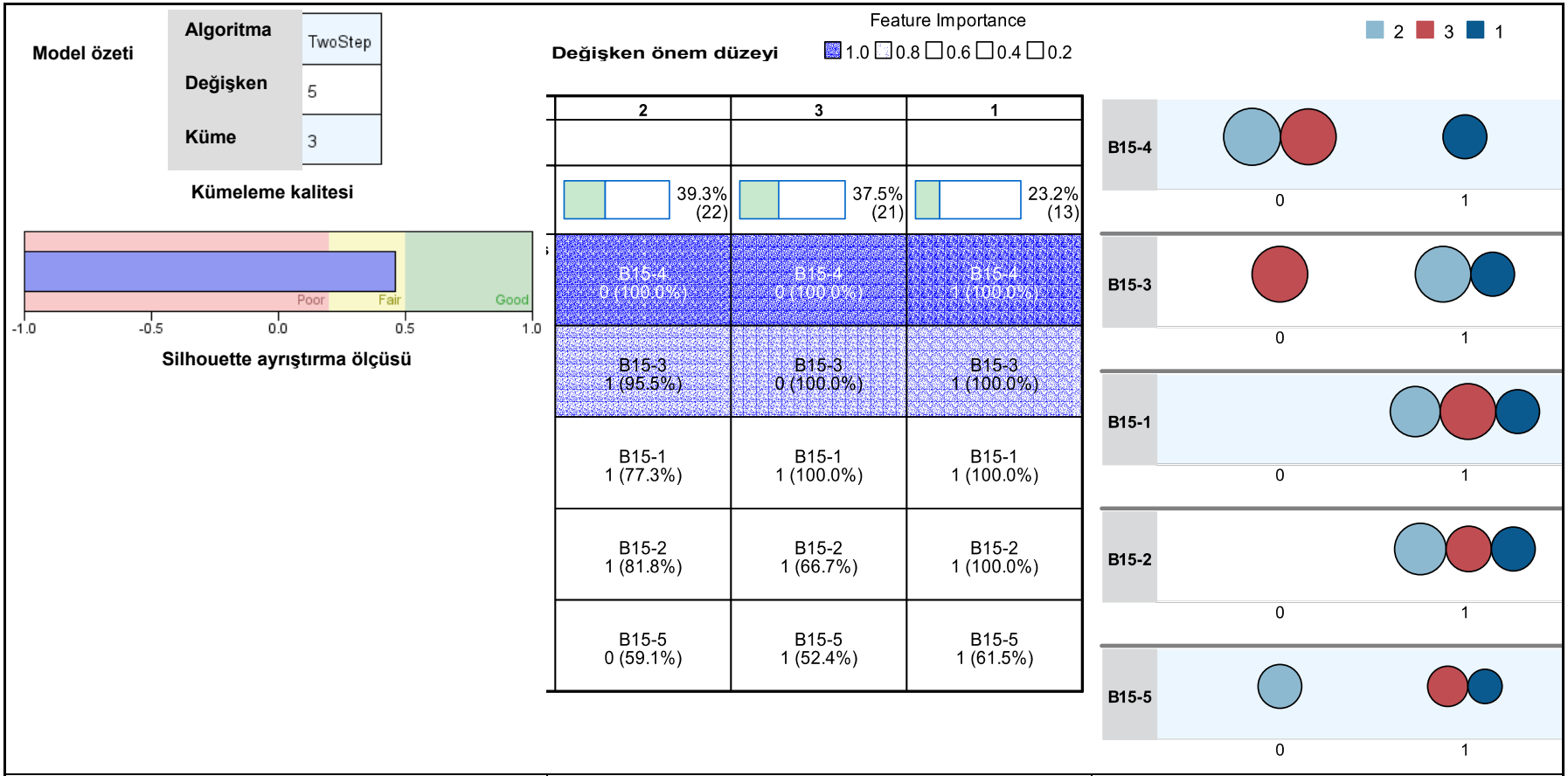
9.7.4. Bilişim teknolojilerindeki güncel teknolojik gelişmelerin takibine göre kümeleme

Kamu kurumlarında çalışan personellerin "bilişim teknolojilerindeki güncel teknolojik gelişmelerin takibi" değişkenine kümeleme analizi uygulandı. Kurumların Bilişim teknolojilerinin takibi konusunda 5 değişken kullanıldı. Benzerlik göstermeleri bakımından 3 grupta kümeleme gerçekleşti. bilişim teknolojilerindeki güncel teknolojik gelişmelerin takibi değişkenine göre yapılan gruplamada orta düzeyde kurumlar arasında benzerlik oluştuğu gözlendi.

Kurumların %39,3'ü ikinci, %37,5'i üçüncü kümede yer aldı. Kümeleme üzerindeki etki dereceleri bakımından değişkenler en önemliden önemsize doğru sıralanmıştır. Bu sıralamada kümelemelerin oluşumunda Bilişim teknolojilerini televizyonlardan takip etme, en önemli değişkeni içerdiği görüldü. Dergi ve gazetelerden öğrenme, benzerlik bakımından ikinci öncelikli sırada yeraldı. Değişkenler önem derecelerine göre azalan sırada, İnternetten ve ilgili sitelerden takip etme, e-posta yolu ile takip etme, Toplantı ve seminerlerden takip etme şeklinde sıralandı.

Bilişim teknolojilerini televizyonlardan takip etme bakımından ikinci ve üçüncü kümede bulunan kurumlar birbirine benzerlik gösterirken çoğunlukla Bilişim teknolojilerini televizyonlardan takip etmeyen kurumlar burada yoğunlaşmıştır. İnternetten ve ilgili sitelerden takip etme değişkeni bakımından ikinci, üçüncü ve birinci küme içinde yer alan kurumlar birbirine benzerlik gösterirken, bilişim teknolojilerine ilişkin yayınları internetten ilgili web sitelerinden öğrenen kurumlar bu kümelerde toplanmıştır. Bilişim teknolojilerini e-posta yolu ile takip etme bakımından iki, üç ve birinci kümeler birbirine benzerlik göstermektedir. Bilişim teknolojilerini toplantı ve seminerlerden takip etme bakımından üçüncü ve birinci kümeler birbirine benzerlik gösterirken, ikinci küme bunlardan ayrılmaktadır.

Kamu kurumları çoğunlukla teknoloji ile ilgili gelişmeleri televizyonlardan takip etmemektedir. Genellikle teknolojik gelişmeleri internetten takip etmektedir.



Küme 2	Küme 3	Küme 1
2 4 11 14 15 33 39 44 47 51 62 63 64 66 68 69 72 73 75 76 80 81	12 16 19 20 26 28 30 35 40 42 43 46 48 52 53 55 60 65 70 71 74	1 7 8 9 22 25 38 29 34 37 61 67 77

Şekil 9.4. Teknolojik Gelişmeleri Takip Şekline Göre Kümeleme

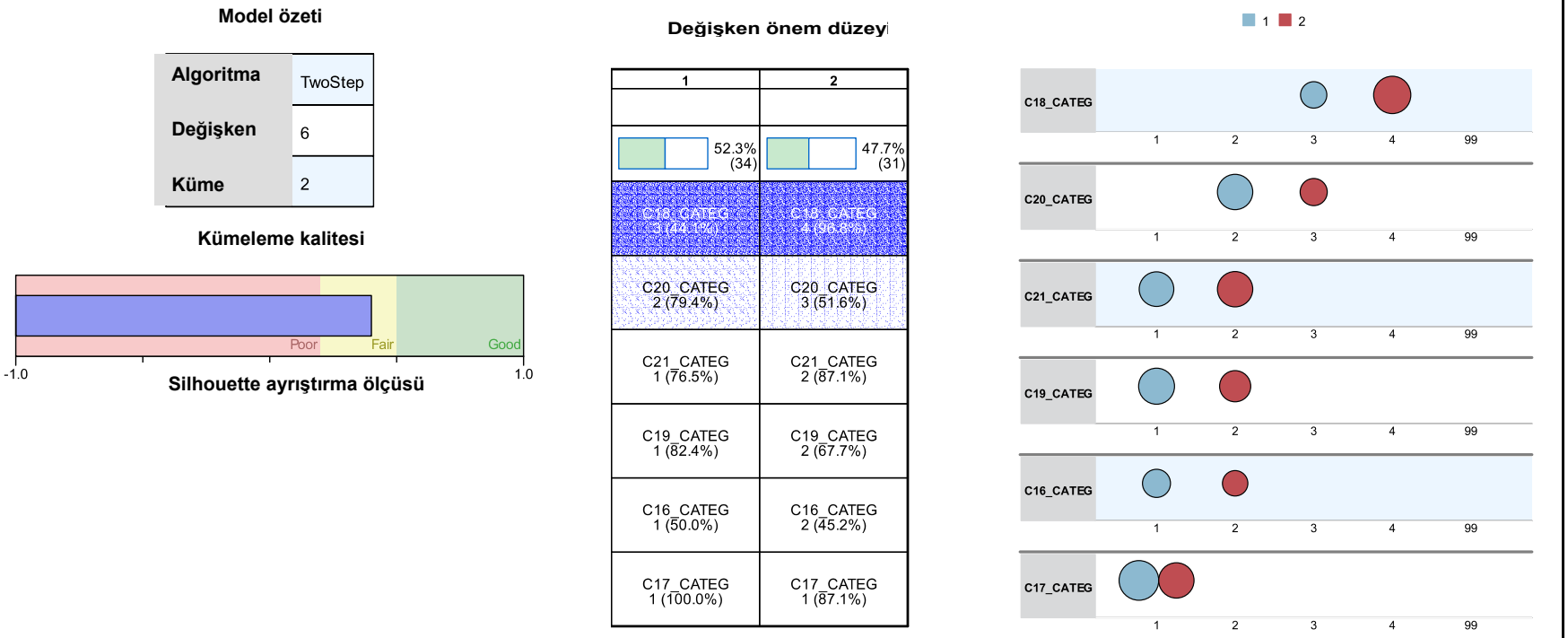
9.7.5. Bilgi işlem merkezlerinin donanım alt yapısına göre kümeleme

Kamu kurumları donanım alt yapısı bakımından, donanım türlerine göre kümeleme analizi uygulandı. Kurumlara donanım ve donanım alt yapısı bakımından 6 değişken kullanıldı. Benzerlik göstermeleri bakımından 2 grupta kümeleme gerçekleşti. Bilgi işlem merkezlerinin donanım alt yapısına göre yapılan gruplamada orta düzeyde kurumlar arasında benzerlik oluştuğu gözlendi.

Kurumların %52,3'ü birinci kümede yer alırken %47,7'si ikinci kümede yer aldı. Değişkenlerin kümelenmesi sonucunda altı değişken en çok benzerlik gösteren değişkenden, en az benzerlik gösteren değişkene doğru sıralandı. Bu sıralamada kümelemelerin oluşumunda kurumlarda kullanılan masa üstü bilgisayar sayısı bakımından en önemli değişkeni içerdiği görüldü. Kurumlarda kullanılan yazıcı sayısı, benzerlik bakımından ikinci öncelikli sırada yer aldı.

Kurumlardaki masaüstü bilgisayar sayısı bakımından birinci ve ikinci kümede bulunan kurumlar birbirine benzerlik göstermemektedir. çoğunlukla donanım alt yapılarından masa üstü bilgisayarlar bakımından kümeler birbirinden ayrıdırlar.

Kurumlarda yazıcı sayısı, tarayıcı sayısı, dizüstü bilgisayar sayısı, sunucu sayısı bakımından birinci ve ikinci kümelerde yer almaktadırlar. Donanım alt yapısındaki aktif cihaz sayıları bakımından birinci ve ikinci küme içinde yer alan kurumlar birbirine benzerlik gösterirken, aktif cihaz sayıları bakımından kurumlar bu kümelerde toplanmıştır. Aktif cihaz bakımından birinci ve ikinci kümeler birbirine benzerlik göstermektedir.



Küme 1	Küme 2
3 6 17 18 19 22 3 25 26 30 33 35 39 41 42 43 46 47 48 49 50 52 53 54 56 60 63 64 65 66 67 74 75 80	2 5 7 9 11 14 15 16 20 24 38 28 32 34 37 40 44 45 51 55 57 58 59 68 69 73 76 77 78 79 81

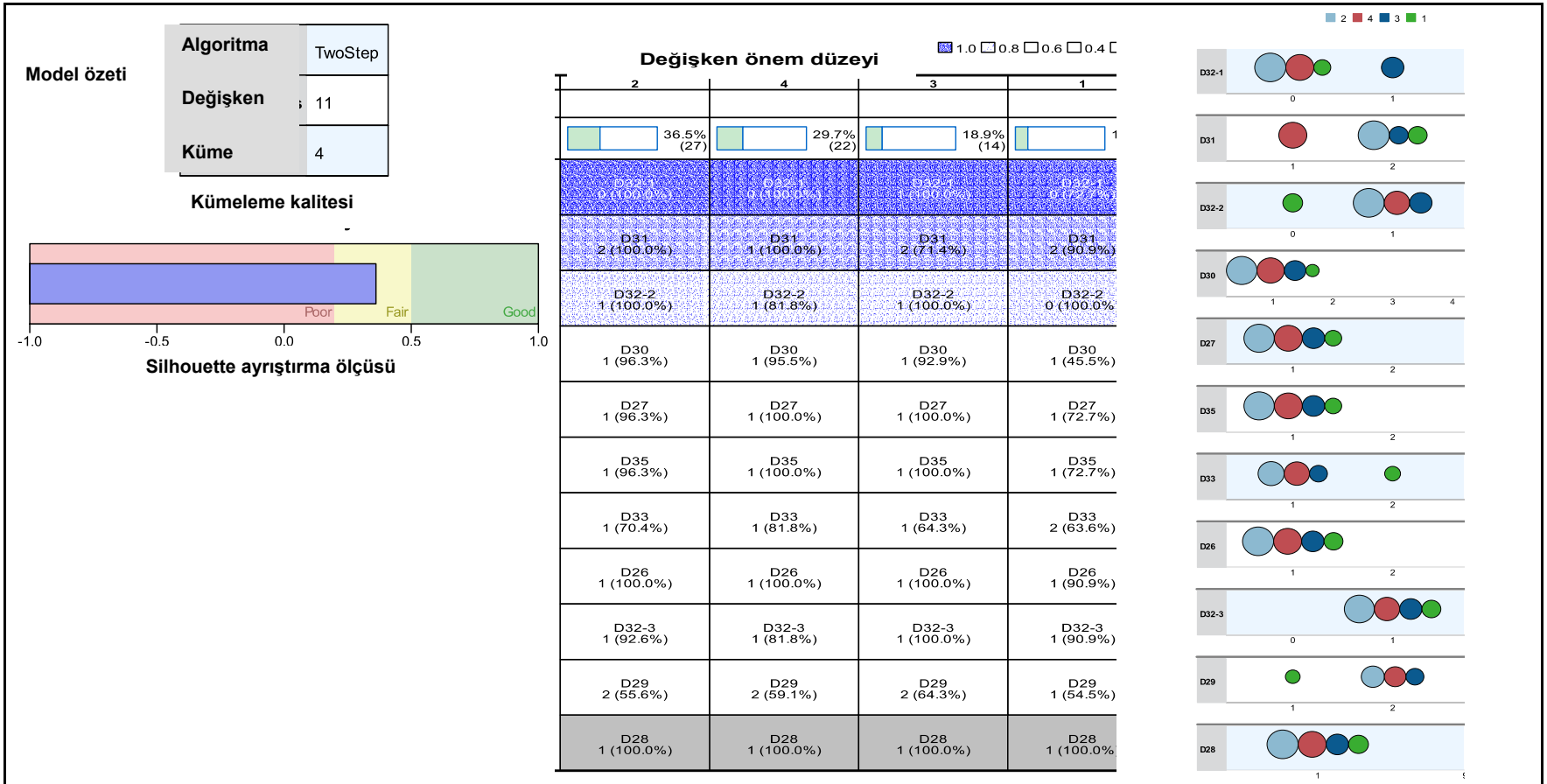
Şekil 9.5. Bilgi İşlem Merkezlerinin Alt Yapısına Göre Kümeleme

9.7.6. Güvenlik alt yapısına göre kümeleme

Kamu kurumlarında Güvenlik alt yapısına göre iki aşamalı küme analizi uygulandı. Kurumlara eğitim sıklığı ve eğitim türü ile ilgili 11 değişken kullanıldı. Benzerlik göstermeleri bakımından 4 grupta kümeleme gerçekleşti. Kümeleme kalitesi orta düzeyde gerçekleşmiştir. Güvenlik alt yapısına göre yapılan gruplamada orta düzeyde kurumlar arasında benzerlik oluştuğu gözlendi.

Kurumların %36,5'i ikinci kümede yer alırken, %29.7'si dördüncü kümede yer aldı. Kümeleme üzerindeki etki dereceleri bakımından değişkenler en önemliden önemsize doğru sıralanmıştır. Bu sıralamada kümelemelerin oluşumunda e-posta kullanımında öncelikli alınan güvenlik önlemlerinden alfa nümerik e-posta şifreleri kullanma değişkeni, verilen eğitim türlerinin içinde en önemli değişkeni içerdiği görüldü. Güvenlik alt yapısında, bilgi güvenliği için kripto kullanımı benzerlik bakımından ikinci öncelikli sırada yer aldı. Güvenlik alt yapısında e-posta şifreleri kullanmak bakımından ikinci, dördüncü ve birinci kümede bulunan kurumlar birbirine benzerlik gösterirken, çoğunlukla e-posta kullanımını tercih etmeyen kurumlar burada kümelenmiştir. Bilgilerin güvenliği için kriptolama kullanımında iki, üç ve birinci kümede bulunan kurumlar birbirine benzerlik gösterirken, çoğunlukla kripto kullanımı tercih eden kurumlar burada kümelenmiştir. Güvenlik alt yapısında güvenlik yazılımlarını kullanmak bakımından ikinci, dördüncü ve birinci kümeler birbirine benzerlik gösterirken, çoğunlukla güvenlik yazılımları tercih etmeleri bakımından kurumlar burada kümelenmiştir.

Birden fazla antivirüs yazılımı kullanmak değişkeni bakımından ikinci, dördüncü ve birinci kümeler birbirine benzerlik göstermektedirler. Çoğunlukla bu değişkeni tercih etmeleri bakımından kurumlar birbirine benzerler. Güvenlik alt yapısı konusunda kurumların tamamı birbirlerine benzerlik göstermektedirler. Bu kümelerde yer alan tüm kurumlar benzer çözüm yollarını tercih etmektedirler.



Küme 2	Küme 4	Küme 3	Küme 1
1 6 12 15 19 21 23 24 25 28 29 35 36 37 39 40 44 49 50 53 56 57 64 71 73 75 79	4 7 11 16 17 38 32 33 43 46 47 51 52 54 59 60 61 62 67 72 74 80	5 14 20 40 42 58 63 65 68 69 70 76 77 81	2 3 9 22 26 27 30 31 34 48 82

Şekil 9.6. Güvenlik Alt Yapısına Göre Kümeleme

9.7.7. Kişisel bilgi güvenliğine göre kümelenme

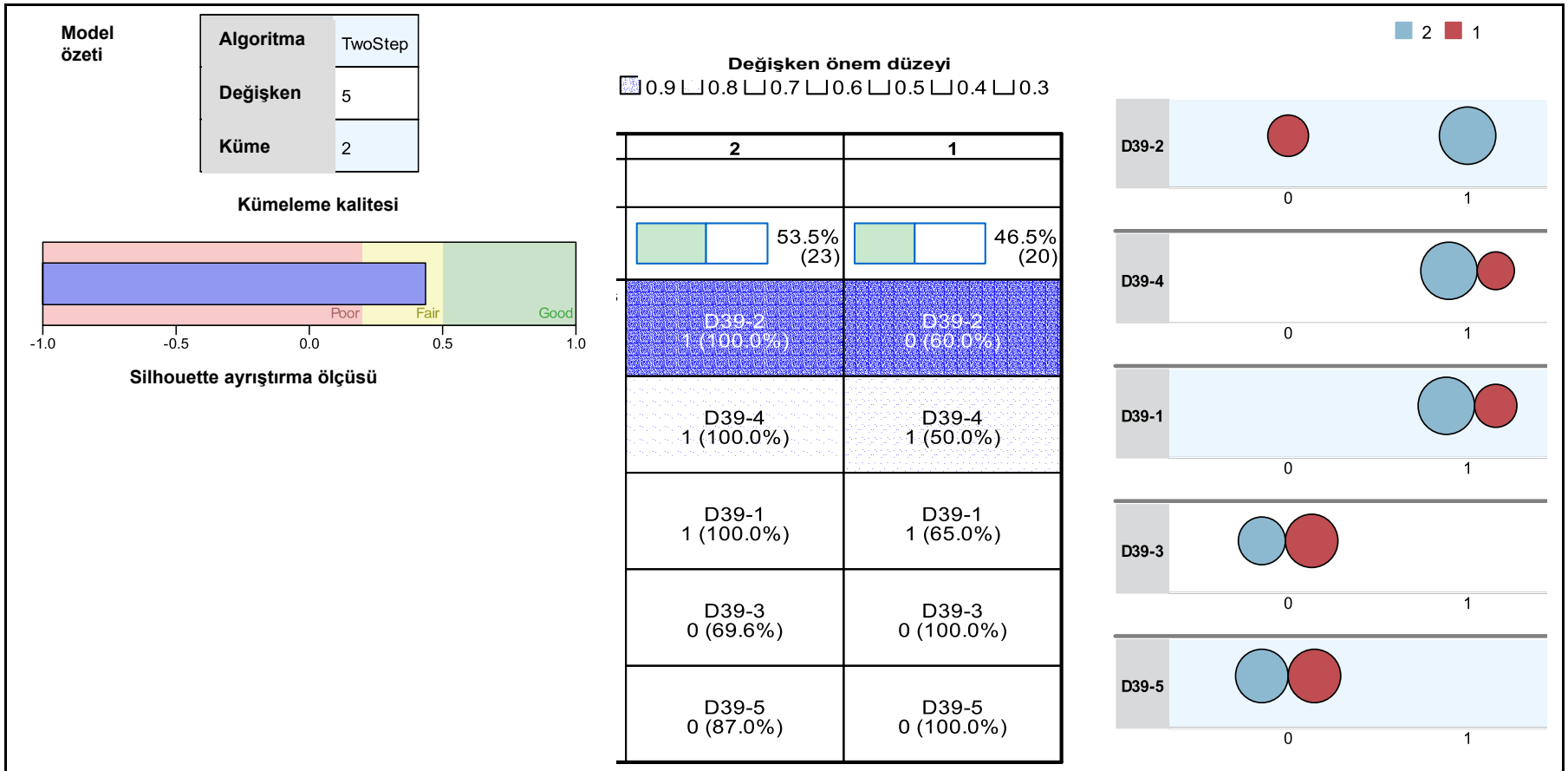
Kamu kurumlarında tutulan kişisel bilgilerin güvenliği bakımından iki aşamalı küme analizi uygulandı. Kurumlardaki bilgi güvenliği ile ilgili 5 değişken kullanıldı. Benzerlik göstermeleri bakımından 2 grupta kümeleme gerçekleşti. Kişisel bilgi güvenliği bakımından, yapılan gruplamada, Kümeleme kalitesi orta düzeyde benzerliklerin oluştuğu gözlendi.

Kurumların %53,5'i ikinci kümede yer alırken, %46,5'i birinci kümede yer aldı. Değişkenlerin kümelenmesi sonucunda beş değişken en çok benzerlik gösteren değişkenden, en az benzerlik gösteren değişkene doğru sıralandı. Bu sıralamada kümelemelerin oluşumunda, Kişisel bilgilerin güvenliğinin sağlanmasında erişimin şifrelerini sınırlandırmak en önemli değişkeni içerdiği görüldü. Kişisel güvenlik bakımından erişim şifrelerini sınırlandırmak, benzerlik bakımından her iki küme, birbirinden farklılık göstermektedir. Değişkenler önem derecelerine göre azalan sırada, Firewall(güvenlik duvarı), veri taşıma sırasında kriptolama, ve diğerleri şeklinde sıralandı.

Uygulama sunucularına kontrollü erişim yetkisi bakımından ikinci ve birinci kümede bulunan kurumlar birbirine benzerlik gösterirken, çoğunlukla uygulama sunucularına kontrollü erişim yetkisi bakımından, kurumlar burada yoğunlaşmıştır. Güvenlik bakımından firewall(güvenlik duvarı) ile kişisel bilgilerin güvenliğinin sağlanması bakımından ikinci ve birinci kümede yer alan kurumlar birbirine benzerlik göstermektedir.

Kişisel bilgilerin güvenliğinin sağlanması açısından, verileri taşıma ve aktarım sırasında kriptolama değişkeni ile uygulama sunucularına kontrollü erişim yetkisi değişkeni bakımından birbirine benzerlik gösterirken, kişisel bilgilerin güvenliği açısından verileri taşıma ve aktarım sırasında kriptolama kullanmayan kurumlarla, uygulama sunucularına kontrollü erişim yetkisi olmayan kurumlar burada yoğunlaştı.

Kişisel bilgi tutan kurumlar daha çok güvenlik duvarı ve kriptolamaya önem verdikleri gözlemlenmektedir.



Küme 2	Küme 1
1 5 7 12 16 20 24 32 33 39 40 50 51 52 55 56 60 63 67 68 69 71 79	6 8 10 11 13 15 22 38 27 43 44 48 49 53 59 65 66 70 72 75

Şekil 9.7. Kişisel Bilgi Güvenliğine Göre Kümeleme

9.7.8. Saldırılardan zarar görme türlerine göre kümeleme

Kurumlarda saldırılar sonucu zarar görme türlerine göre iki aşamalı küme analizi uygulandı. Saldırı sonucu zarar görme türleri bakımından 5 değişken kullanıldı. Benzerlik göstermeleri bakımından 4 grupta kümeleme gerçekleşti. Kurum bilgi işlem merkezlerine yapılan saldırı sonucunda zarar görme türlerine göre yapılan Gruplamada, kümeleme kalitesi iyi biçimde gerçekleşmiştir.

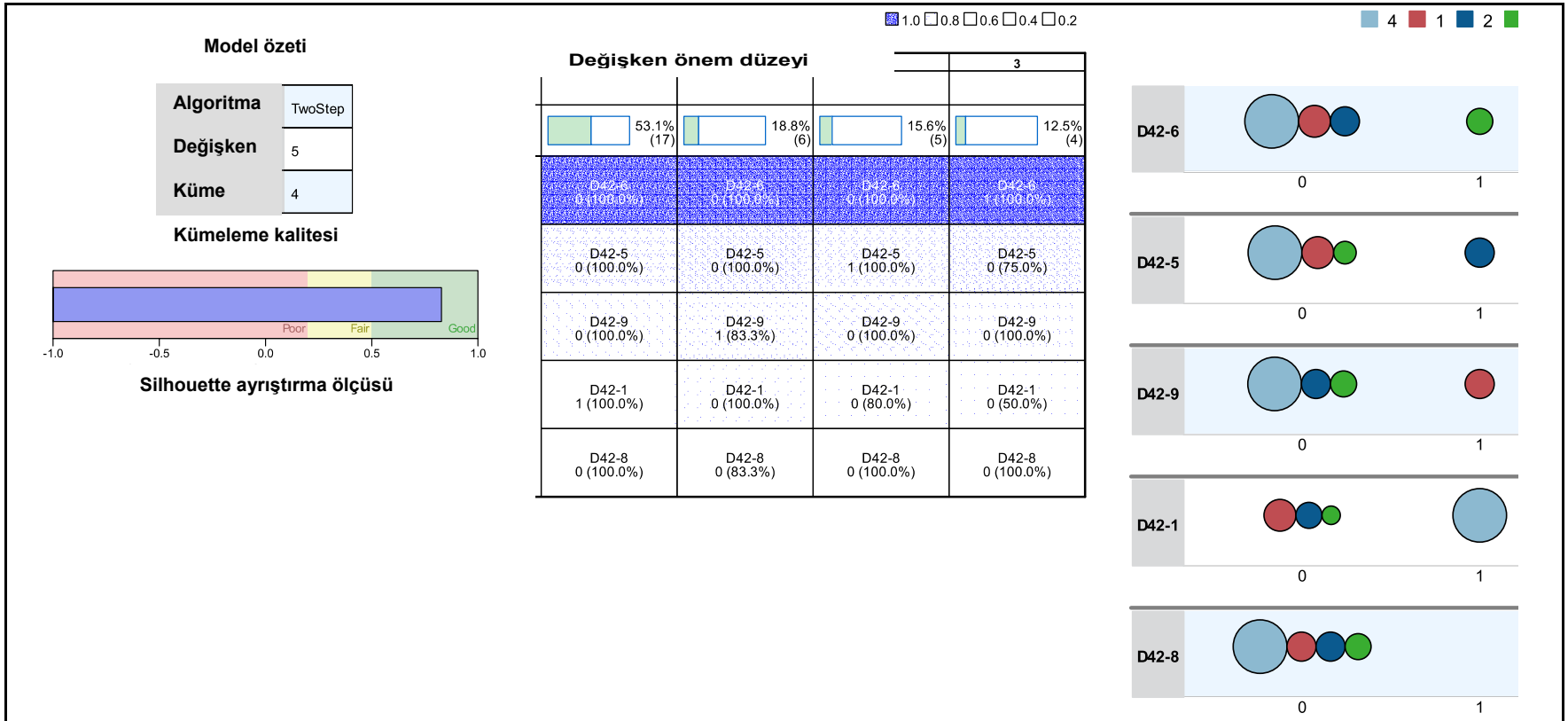
Kurumların %53,1'ü dördüncü kümede yer alırken, %18,8'i birinci kümede, %15,6'sı ikinci kümede %12,5'i üçüncü kümede yer aldı. Değişkenlerin kümelenmesi sonucunda beş değişken en çok benzerlik gösteren değişkenden, en az benzerlik gösteren değişkene doğru sıralandı. Bu sıralamada kümelemelerin oluşumunda, sistemlerin saldırı sonucu zarar görme türleri arasında ağ erişimlerinin engellenmesi en önemli değişkeni içerdiği görüldü. Saldırıda zarar görme türleri içinden e-posta erişimi ikinci öncelikli sırada yer aldı. Değişkenler önem derecelerine göre azalan sırada, saldırı sonucu herhangi bir zarar görmediği, Web sayfası çalışamaz duruma getirilmesi, verilerin içeriğinin değiştirilmesi şeklinde sıralandı.

Zarar türlerinden ağ erişimini engelleme türleri bakımından dördüncü, birinci ve ikinci kümede bulunan kurumlar birbirine benzerlik gösterirken çoğunlukla ağ erişiminin engellenmesi bakımından zarar görmeyen kurumlar burada yoğunlaşmıştır.

Saldırı sonucu zarar görme seçenekleri bakımından e-posta erişiminin engellenmesi türü bakımından dördüncü, birinci ve üçüncü kümede bulunan kurumlar birbirine benzerlik gösterirken çoğunlukla e-posta erişiminin engellenmesi bakımından zarar görmeyen kurumlar bu kümelemede yoğunlaşmıştır. Saldırı sonucu herhangi bir zarara uğramamaları bakımından dördüncü, ikinci ve üçüncü kümede bulunan kurumlar birbirine benzerlik gösterirken, çoğunlukla herhangi bir zarar görme bakımından kurumlar bu kümelemede yoğunlaşmıştır.

Saldırı sonucu web sayfasını çalışamaz duruma getirilmesi bakımından birinci, ikinci ve üçüncü kümede yer alan kurumlar birbirine benzerlik gösterirken çoğunlukla web sayfasını çalışamaz duruma getirilmesi bakımından zarar görmeyen kurumlar bu kümelemede yoğunlaşmıştır.

Saldırı sonucu önemli zarar türlerinden, verilerin içeriğinin değiştirilmesi bakımından dördüncü, birinci, ikinci ve üçüncü kümede yer alan kurumlar birbirine benzerlik göstermektedir. Çoğunlukla verilerin içeriği değiştirilmemesi bakımından kurumlar bu kümelerde yoğunlaşmıştır.



Küme 4	Küme 1	Küme 2	Küme 3
6 9 10 11 12 14 15 16 19 38 27 29 40 43 53 69 74	1 18 25 32 44 70	42 56 73 76 80	20 24 54 66

Şekil 9.8. Saldırıdan Zarar Görme Türüne Göre Kümeleme

9.7.9. Bilgi işlem merkezlerinin fiziksel güvenliğine göre kümeleme

Bilgi işlem merkezlerinin fiziksel güvenliği bakımından iki aşamalı küme analizi uygulandı. Kurumlara fiziksel güvenlikle ilgili 9 değişken kullanıldı. Benzerlik göstermeleri bakımından 5 grupta kümeleme gerçekleşti. Fiziksel güvenlik ile ilgili orta düzeyde, kurumlar arasında benzerlik oluştuğu gözlendi.

Kurumların %36,2'si birinci kümede yer alırken, %17,5'i beşinci kümede yer aldı. Değişkenlerin kümelenmesi sonucunda dokuz değişken en çok benzerlik gösteren değişkenden, en az benzerlik gösteren değişkene doğru sıralandı. Bu sıralamada kümelemelerin oluşumunda bilgi işlem merkezlerinin sistem odalarına girişlerde parmak izi kullanımı değişkeni, benzerlik bakımından en öncelikli sırada yer aldı. öncelikli önem derecelerine göre azalan sırada, bilgi işlem merkezlerine "giriş çıkışlarda kartlı sistemlerle" seçeneği önem derecesi en yüksek derecede sıralandı.

Sistem odasına girişlerde parmak izi kullanımı bakımından birinci, beşinci, ikinci ve dördüncü kümelerde bulunan kurumlar birbirine benzerlik gösterirken çoğunlukla sistem odasına parmak izi kullanmadan geçişler bakımından kurumlar burada yoğunlaşmıştır. Sistem odasına girişlerde diğer seçeneği bakımından, birinci, ikinci, üçüncü ve dördüncü kümelerde bulunan kurumlar birbirine benzerlik gösterirken, çoğunlukla diğer seçeneğini kullanmayan kurumlar burada yoğunlaşmıştır.

Sistem odasına girişlerde tuş takımı üzerinden şifre girerek, bakımından birinci, beşinci, üçüncü ve dördüncü kümelerde bulunan kurumlar birbirine benzerlik gösterirken çoğunlukla sistem odasına tuş takımı kullanmadan girenler bakımından kurumlar burada yoğunlaşmıştır.

Sistem odasına girişlerde kartlı sistemi kullanmak bakımından beşinci ve üçüncü kümelerde bulunan kurumlar birbirine benzerlik gösterirken,çoğunlukla çoğunlukla kartlı sistemi kullanmayanlar bakımından kurumlar burada kümelenmiştir, birinci, ikinci ve dördüncü kümelerde bulunan kurumlarda kartlı sistemlerle geçiş

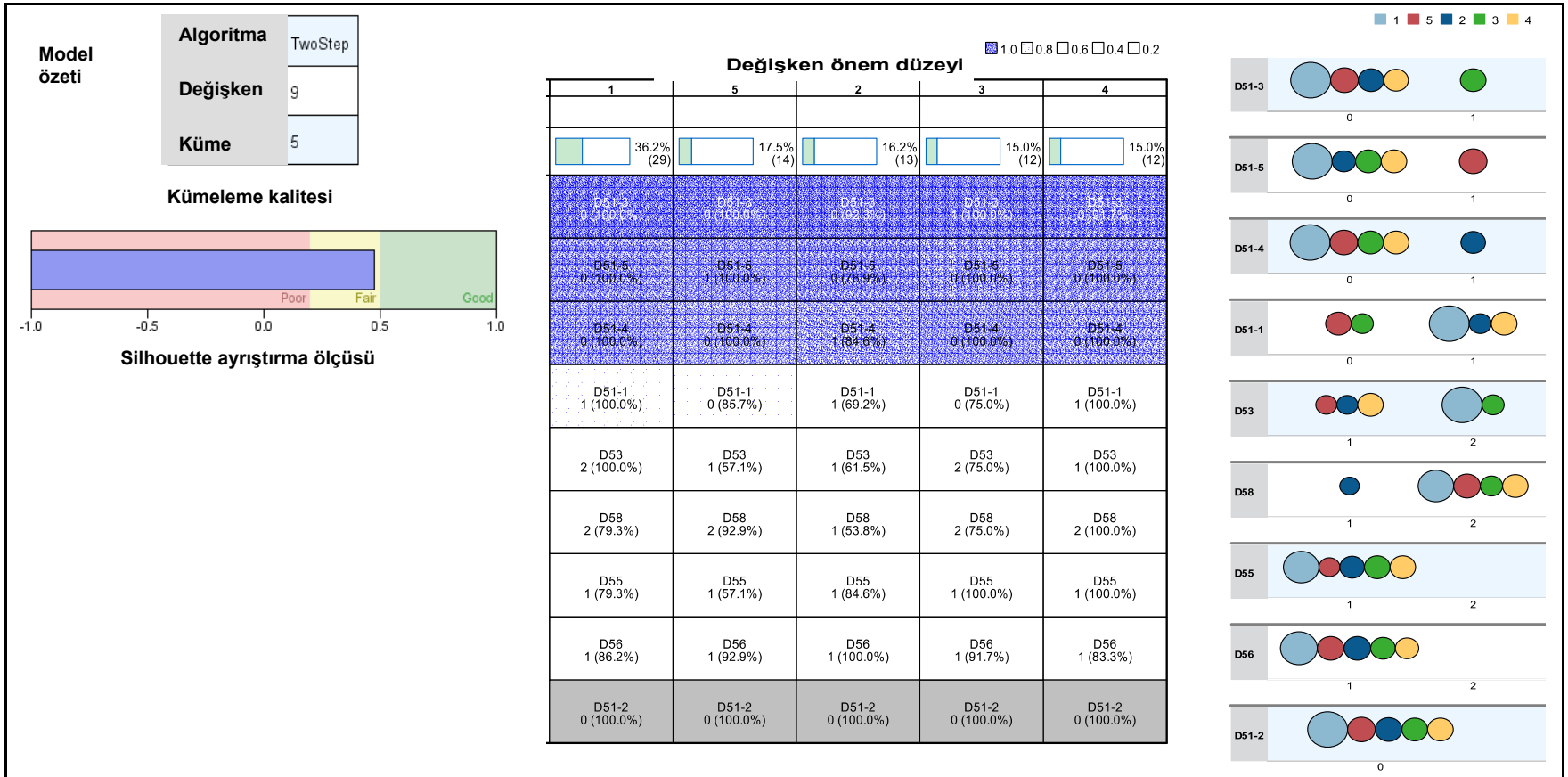
bakımından birbirine benzerlik göstermektedir. Çoğunlukla kartlı sistemleri kullanan kurumlar burada kümelenmiştir.

Bilgi işlem merkezlerine giriş çıkışlar konusunda beşinci, ikinci ve dördüncü kümeler birbirine benzerlik göstermektedir. Çoğunlukla bilgi işlem merkezlerine giriş ve çıkışlar açık olan kurumlar burada kümelenmiştir. Bilgi işlem merkezine giriş çıkışlar bakımından bir ve üçüncü kümelerde bulunan kurumlarda bir birine benzerlik göstermektedir. Çoğunlukla giriş ve çıkışlar bakımından kurumlar burada kümelenmiştir.

Sistemin bir yedeğinin başka bölgede (disaster recovery) bulunması bakımından birinci, beşinci, üçüncü ve dördüncü kümelerde bulunan kurumlar birbirlerine benzerlik göstermektedirler. Çoğunlukla disaster recovery merkezi bulunması bakımından kurumlar burada kümelenmiştir.

Sistem odalarını yangın sisteminin olup olmadığı, güvenlik kamerasının bulunup bulunmadığı bakımından, birinci, beşinci, ikinci, üçüncü ve dördüncü kümelerde bulunan kurumlar birbirine benzerlik göstermektedir. Çoğunlukla sistem odalarında yangın sistemi ve güvenlik kamera sistemi bulunması bakımından kurumlar burada kümelenmiştir.

Bilgi işlem merkezlerindeki sistem odalarına giriş çıkışlarda güvenlik nedeniyle göz izi değişkeni bakımından birinci, beşinci, ikinci, üçüncü ve dördüncü kümelerde bulunan kurumlar birbirlerine benzerlik göstermektedirler. Çoğunlukla sistem odalarına giriş çıkışlarda göz izi kullanılmaması bakımından kurumlar burada kümelenmiştir.



Küme 1	Küme 5	Küme 2	Küme 3	Küme 4
1 3 4 5 7 8 9 12 14 16 19 21 22 26 27 30 31 34 47 55 67 68 69 70 71 72 74 75 81	15 18 25 26 27 37 46 48 49 50 57 60 63 65	20 38 32 36 41 43 51 53 54 58 61 64 77,	3 13 31 33 40 44 45 56 62 73 78 79	2 6 17 24 28 39 42 52 59 66 76 80

Şekil 9.9. Bilgi İşlem Merkezlerinin Fiziksel Güvenliğine Göre Kümeleme

9.7.10. Yazılı güvenlik talimatına göre kümelenme

Kurumlar bilgi işlem merkezlerinde herhangi bir zamanda doğacak felaket için yazılı bir güvenlik talimatı bulundurmalıdır. Bilgi işlem merkezleri yazılı güvenlik talimatı bakımından kümeleme analizine tabii tutulmuş, 4 değişken kullanılmıştır. Benzerlik göstermeleri bakımından 2 grupta kümeleme gerçekleşmiştir. Yazılı bir güvenlik talimatı bulundurma bakımından yapılan kümelemenin iyi bir düzeyde yaklaşmış olduğu gözlendi.

Gerçekleşen 2 küme incelendiğinde Kurumların %51,2'si birinci kümede yer alırken, %48,8'i ikinci kümede yer aldı. Değişkenler birbirlerine benzerlik göstermeleri bakımından, seçilen dört değişken en çok benzerlik gösteren değişkenden en az benzerlik gösteren değişkene doğru sıralanmıştır. Bu sıralamada kurumların yazılı bir güvenlik politikası dokümanı bakımından en belirgin kümelemeye sahip değişken olduğu görüldü.

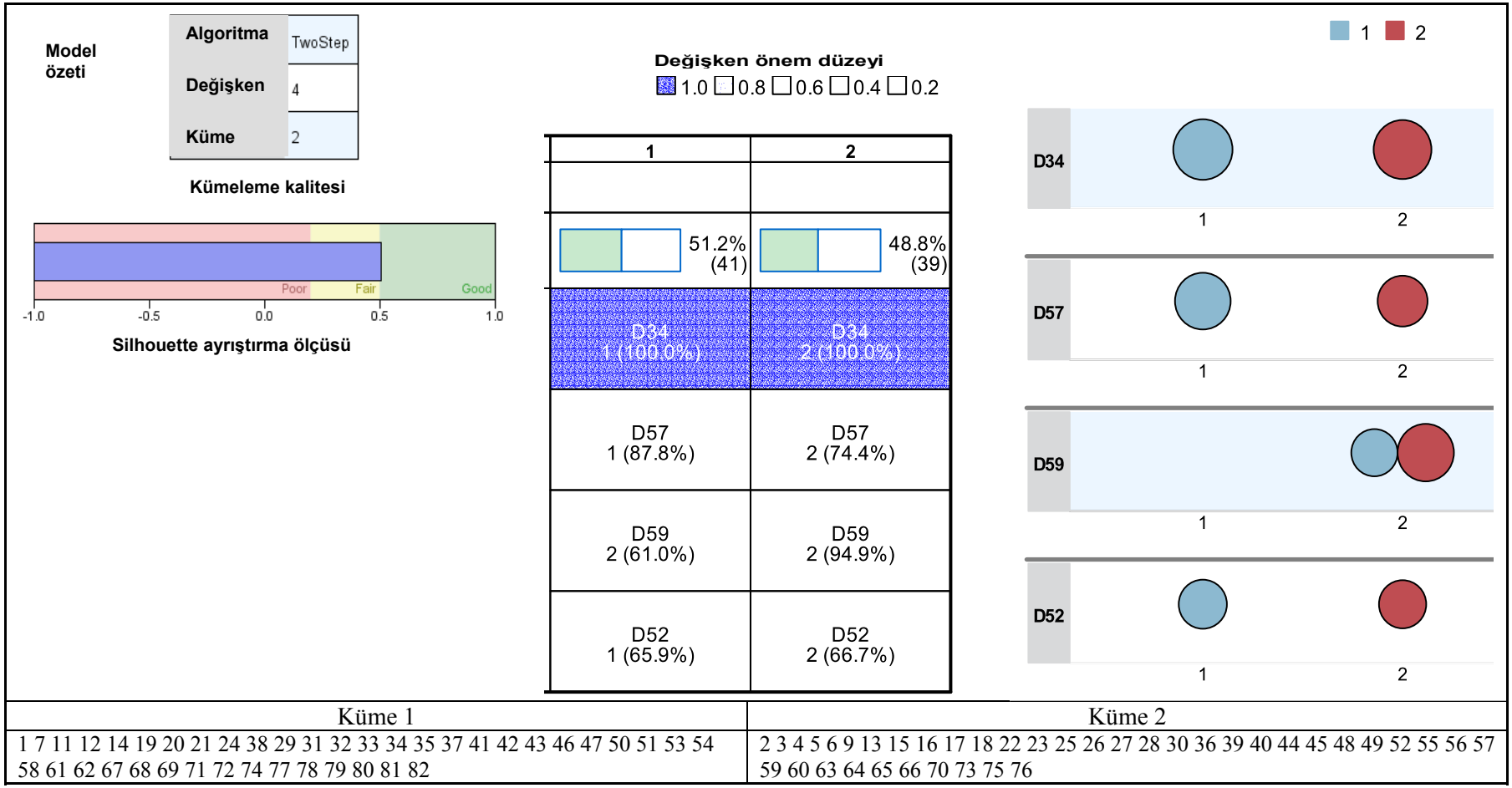
Çoğunlukla yazılı bir güvenlik politikası dokümanına sahip kurumlar burada kümelendi. Kurumlar uygulamakta olduğu yazılı güvenlik standardının bulunması bakımından birbirine benzeyen kümeler sıralamasında ikinci önemli değişkeni oluşturdu.

Kurumların yazılı güvenlik politikası bakımından birinci küme de bulunan kurumlar kendi içinde benzerlik gösterirken, ikinci küme içinde bulunan kurumlarda kendi içerisinde benzerlik göstermektedir. çoğunlukla yazılı güvenlik politikası olan kurumlar burada kümelenmiştir.

Yazılı güvenlik standardı bakımından kurumlar birinci kümede kendi içinde birbirine benzerlik gösterirken, ikinci kümedeki kurumlarda kendi içlerinde birbirine benzerlik göstermektedir.

Kurumların bilgi işlem merkezlerinde yazılı felaket senaryosu bulunması bakımından incelendiğinde burada oluşan kümelerin tamamı birbirine benzerlik göstermektedir.

Ve çoğunlukla birinci ve ikinci kümelerdeki kurumların bilgi işlem merkezlerinde yazılı felaket senaryosu bulunmaktadır. Sistem odası acil durum yönetim yazılı talimatı bakımından birinci kümede bulunan kurumlar kendi içlerinde benzerlik gösterirken, ikinci kümede bulunan kurumlarda kendi içlerinde benzerlik göstermektedir. Çoğunlukla birinci ve ikinci kümelerdeki kurumlar kendi içlerinde, birbirine benzer sistem odalarında acil durum yönetimi için yazılı talimatları bulunmaktadır.



Küme 1	Küme 2
1 7 11 12 14 19 20 21 24 38 29 31 32 33 34 35 37 41 42 43 46 47 50 51 53 54 58 61 62 67 68 69 71 72 74 77 78 79 80 81 82	2 3 4 5 6 9 13 15 16 17 18 22 23 25 26 27 28 30 36 39 40 44 45 48 49 52 55 56 57 59 60 63 64 65 66 70 73 75 76

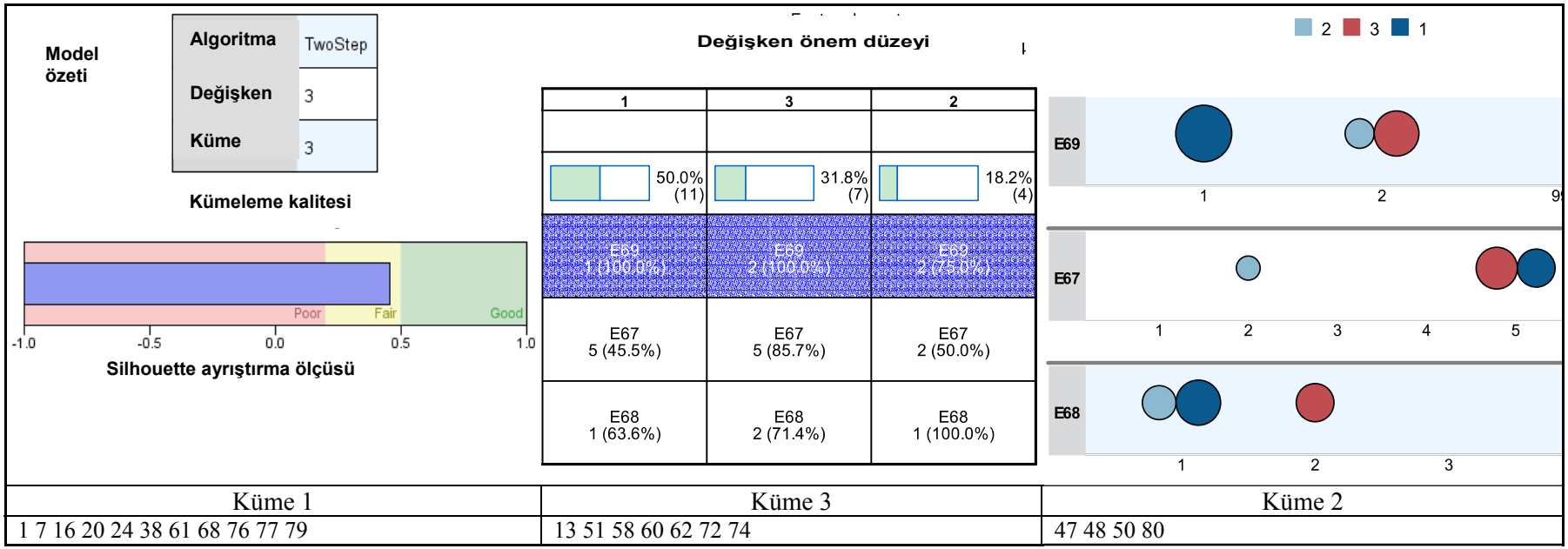
Şekil 9.10. Yazılı Güvenlik Talimatına Göre Kümeleme

9.7.11. E-imzaya göre kümeleme

5070 sayılı e-imza kanununun yürürlüğe girmesi ile kurumlar alt yapı çalışmalarını başlatmış belli aşamalara gelmişlerdir. Kurumların e-imza çalışmalarında geldiği aşamaları tespit etmek bakımından kümeleme analizine tabi tutulmuş, 3 değişken kullanılmıştır. Benzerlik göstermeleri bakımından 3 grupta kümeleme gerçekleşmiştir. E-imza kullanımı ve gelinen aşamaları tespit etmek bakımından yapılan kümelemenin orta düzeyde bir kümeleme olduğu gözlendi.

Gerçekleşen 3 küme incelendiğinde Kurumların %50'si birinci kümede yer alırken, %31,8'i üçüncü kümede, %18,2'si ikinci kümede yer aldı. Değişkenler birbirlerine benzerlik göstermeleri bakımından, seçilen üç değişken en çok benzerlik gösteren değişkenden en az benzerlik gösteren değişkene doğru sıralanmıştır. Bu sıralamada, kurumların e-imza konusunda danışmanlık destek alması bakımından kümelemeye sahip en belirgin değişken olduğu görüldü. E-imza konusunda danışmanlık desteği alması bakımından ikinci ve üçüncü kümeler birbirine benzerlik gösterirken, çoğunlukla e-imza desteği alan kurumlar burada yoğunlaşmıştır. Birinci küme bunlardan ayrılmıştır.

E-imza uygulamalarını hangi aşamada olduğu bakımından üçünü ve birinci kümeler birbirine benzerlik gösterirken, çoğunlukla e-imza uygulamaları konusunda kurumlar burada yoğunlaşmıştır. Kurum içi veya kurum dışı uygulamalarda e-imza kullanımı bakımından ikinci ve birinci kümeler birbirine benzerlik gösterirken, çoğunlukla kurum içi ve kurum dışı e-imza uygulamaları konusunda kurumlar burada yoğunlaşmıştır. Üçüncü kümede yer alan kurumlar diğerlerinden ayrılmıştır. E-imza konusunda kurumlar istenilen seviyeye gelememiştir. Çok az sayıda kurum elektronik imza uygulamalarını başarıyla tamamlamıştır.



Küme 1	Küme 3	Küme 2
1 7 16 20 24 38 61 68 76 77 79	13 51 58 60 62 72 74	47 48 50 80

Şekil 9.11. E-imzaya Göre Kümeleme

10. SONUÇ VE ÖNERİLER

Kamu kurumlarına uygulanan anket sonucunda, birtakım sonuçlar ortaya çıkmıştır. Bu sonuçlardan, ortaya çıkan duruma göre, bir takım önerilerde bulunulmuştur.

10.1. Sonuçlar

Kurumların bilgi işlem merkezlerinin idari yapısı bakımından incelendiğinde belli bir standardın sağlanmadığı, idari yapıda sekizden fazla oluşumun var olduğu gözlenmiştir. Dolayısı ile başta idari yapı olmak üzere, standardın sağlanması ve kalitenin yakalanması için, kurumların tamamının aynı yapı içinde hareket etmesi gerekmektedir. Bu birliktelik sorunların çözümünde maliyet, zaman açısından kazanç sağlayacağı gibi kalite bakımından da belli bir seviyeyi yakalayacaktır.

Araştırma sonuçlarına bakıldığında, Kamu kurumlarındaki Bilgi İşlem merkezlerinin %41,5 i daire başkanlığı olarak faaliyet göstermektedir. %18,3 ü başka birimler altıda şube müdürlüğü olarak faaliyet gösterirken, bu durum kamuda bir standardın olmadığını görülmektedir.

Yapılan araştırmanın sonucuna göre, kurumların %52,4'ünün aktif kullanıcı sayısı 1000 ve daha az olarak tespit edilmiştir. Bilgi işlem merkezlerinde çalışanların yoğunluğunun 10-30 aralığında olduğu, çalışanların %67'sinin eğitim düzeylerinin lisans düzeyinde olduğu görülmektedir. Bilgisayar güvenliği bilinçlendirme eğitimi alan kurumlar %64,6 olmasına rağmen eğitimin amaca ulaşmadığı, verilen eğitimlerin sıklıklarına bakıldığında büyük çoğunluğunun ancak yılda bir defa eğitim verdiği görülmektedir. Verilen eğitim türleri içerisinden kurumların çoğunluğu bilgisayar temel eğitimi vermişlerdir.

Kurumların %97,6'sında internet hizmetleri verilmektedir. Alınan bu internet hizmetleri içinden kurumların Metro ethernet bağlantısını tercih ettikleri görülmektedir. İnternet çıkışlarını ağırlıkta yüksek kapasitede tercih etmektedirler. Kurum çalışanlarının %93,75'i internet hizmetlerinden yararlanmaktadırlar. İnternet

bağlantısından kaynaklanan sorunlar nedeni ile ilgili sorulan sorulara kurum kullanıcılarının verdikleri cevaplarda %76,3'oranında istenmeyen e-posta iletilerinden rahatsızlık duydukları gözlenmiştir. Kurum çalışanlarına internet sınırlı olarak kullandırılmakta, bazı sakıncalı görülen siteler uygulamaları engelleyeceği düşüncesiyle yasaklanmaktadır.

Bilgi işlem çalışanları, bilgi teknolojileri ile ilgili sürekli yayın takip etmekte, ve bu yayınların büyük çoğunluğunu internet üzerinden, web sitelerinden takip ettikleri gözlenmektedir. Kurumlar donanım bakımlarının %35,7'sini kendi imkanlarıyla yapmaktadır. BİM'lerin %72'sinin kurumlarından yeterli teknik destek aldıklarını ifade etmişlerdir.

Kurum bilgi işlem merkezlerine, bilgi güvenliği ve fiziksel güvenlik konusunda, %98,8'inin güvenlik yazılımı kullandığı, %95'inin bu güvenlik yazılımının üzerine yükleneceği güvenlik donanımları bulunmaktadır. Kurumların %39,5'inin güvenlik için ikinci bir antivirüs yazılımın olduğu, %86,6'sının kullandıkları anti virüs programı güncellemelerinin yapıldığını .gözlenmiştir.

Güvenlik konusun da önemli bir unsur olan kriptolamaya çok fazla itibar edilmediği, ancak cevap veren kurumların %37,5'i kripto kullandıklarını söylemişlerdir. Kurumların %46,5'i e-posta kullanımında güvenlik önlemi olarak antivirüs yazılımını öncelikle tercih etmişlerdir. %36,3'ünde saldırı tespit sistemlerinin bulunmamakta, %48,8'inde ise kurumlarında yazılı bir güvenlik politikaları bulunmamaktadır. Kurumların tamamına yakını sakıncalı siteleri filitrelemekte ve sistemlerini yedeklerini almaktadırlar. Yedekleme alan bu kurumların %82,7'si hergün yedekleme almaktadırlar.

Kurumların ancak % 52,4'ünde kişisel bilgiler tutulmaktadır. Kişisel bilgilerin güvenliğini sağlarken, kurumlar kişisel bilgilerin bulunduğu sunuculara kontrollü erişim ve firewall 'u (güvenlik duvarı) çoğunlukla tercih etmişlerdir. %84,1'inin ise saldırı tespiti izleme yaptığı görülmektedir.

Kurumların %39'una saldırıda bulunulmuş, saldırı sonucunda %62,5 oranında web sayfası çalışamaz duruma getirilmiştir. Ayrıca e-posta erişimleri engellenmiş, %2,8'inin verilerinin içeriği değiştirilmiştir. %13,9 ise saldırıya uğramalarına rağmen herhangi bir zarara uğramamıştır. Saldırıya uğrayan kurumların %83,33'ü manevi zararlarının, maddi zararlardan daha fazla olduğunu görülmektedir. Kurumlar bilgi işlem merkezlerinde, güvenlik denetimi yaparken, hemen hepsi domain yapısına sahip olduklarını ifade etmişlerdir. Bilgi alış verişi için bazı kurumlar aralarında bağlantı kurmuşlardır. %62,2'si bu bağlantıya sahiptir. Bağlantı sağlanan bu kurumların ise %98,04'ü çift yönlü bağlantıya sahiptir. %85,4'ünde aktif directory yapısı mevcuttur.

Kurumlarda kullanıcıların %96,3'ü kendi şifreleri ile sisteme bağlanmaktadır. Fiziksel olarak sistem odalarına girişleri ise, büyük çoğunlukla manyetik kart kullanarak yapmaktadır. Sistem odalarının güvenliği için %50'sinin yazılı güvenlik talimatı bulunmamaktadır. Bilgi işlem merkezlerine girişlerde güvenlik önlemleri kurumların %39'unda sağlanmaktadır. Kurumların %17,8'inde yangın söndürme sistemi bulunmamaktadır. Büyük bir kısmında bina güvenlik kamera sistemleri bulunmaktadır. Kurumlar sistemlerinin herhangi bir felaket anında zarar görmemesi için başka bölgelerde bir yedeğini tutmaktadırlar, kurumların %22'sinin başka bölgelerde yedekleri bulunurken, yazılı felaket senaryosu da bulunmaktadır.

Kurumların %96,3'ü açık kaynak kodlu programları kullanmaktadırlar. Bu kaynak kodlarından en çok kullanılan Linux ve Open Office yazılımlarıdır. Kurumların %57,3'ü e-devlet uygulamalarının olduğunu ifade ederken, %26,8'i elektronik imza kullandıklarını söylemişlerdir. E-imza kullanan kurumların %54,55'i kurumlarını iç yazışmalarında kullandıklarını ifade etmişlerdir.

Yöneticilerin bilişim teknolojilerine yaklaşımları araştırılmış, %41,5'inin teknolojik açıdan çalışanlarına destek verdiği fakat yeterli desteği vermediği belirtilmiştir. Sunucularda tutulan bilgilerin güvenliği ve hukuki sorumlulukları konusunda sorulan sorulara, %85,4 oranında sunucuların güvenli olduğunu ve %90,24 oranında hukuki sorumluluklarını bildiklerini belirtmişlerdir. Bilgi işlem çalışanlarının %92,7'sinin

çalıştıkları ortamlardan memnun olduklarını ifade etmelerine rağmen %81,7'si aldıkları maaşların memnuniyet verici olmadığını ifade etmişlerdir.

İdari yapısı Genel müdürlük olan kurumlarda eğitim alma oranının diğer birimlere göre daha fazla olduğu ve arasıra eğitim aldığı görülmektedir. Kurumlar genellikle eğitimlerini yılda bir defa planlamaktadır. Toplamda kurumların %43,4'ü yılda bir defa eğitim almaktadırlar. İdari birimlerdeki kullanıcı sayısına bakıldığında personel yoğunluğunun, müdürlüklerde ve daire başkanlıklarında yoğunlaştığı görülmektedir. Bu yoğunluk müdürlüklerde 100-500 personel aralığında %41,9'unu oluştururken, Daire başkanlıklarında kullanıcı sayıları 1000'den daha fazla personele sahip ve %58,8'ini oluşturmaktadır. İdari birimlerin yapılarıyla, kullanıcı sayısı arasında da anlamlı bir ilişki olduğunu söylemek mümkündür.

Bilişim güvenliğine yönelik bilinç ve duyarlılığın düzeyi ile kamu bilgi işlem uygulamalarının güvenlik açısından durumunu belirlemek için anket sonuçları genel anlamda aşağıdaki maddeler şeklinde yorumlanabilir.

- Kamu'nun bir çok biriminde bilişim sistemlerinin bilgi düzeyi yetersiz personel ile işletildiği,
- Personel eğitim gereksinimlerinin olduğu,
- Sistem odalarının yeterli fiziksel güvenlik gereklerini karşılamadığı,
- Bilişim güvenliğinden sorumlu bir birimin olmadığı,
- Uygulanan güvenlik politikaları ve standartlarının olmadığı,
- Dışarıdan gelecek tehditlere karşı firewall ile önlem almaya çalıştıkları,
- Bilgilerin önem derecelerinin belirlenmediği,
- Güvenli işletim sistemleri konusunda yeterli bilgileri olmadığı,
- Erişim kontrolünün çok fazla ciddiye alınmadığı,
- Sistemi sürekli izleme alışkanlıklarının olmadığı,
- Sistem güvenlik loglarının arşivlenmediği,
- Sistem kaynaklarının denetime alınmadığı,
- Virüs temizleme programlarının yeni sürümlerini elde etme zorluğu,

- Beklenmedik durum planlarının olmadığı tespit edilmiştir,

Kamuya ilişkin bir bilişim güvenliği politikası ve Ulusal Bilgi güvenliğine yönelik bir politikaları belirleyecek, standartları koyacak ve gerektiğinde denetimleri sağlayacak bir kurum henüz oluşmamıştır.

Bilgi güvenliğine yönelik bir standardın da henüz olmadığı, bir İngiliz standardından çevrilmiş TSE nin standart olarak kabul gördüğü TSE, ISO-27001 güvenlik standardının, TSE standardı olarak yayınlanması uygun bulunmuştur [Türk Standartları Enstitüsü ISO-27001, 2006].

10.2. Öneriler

Kamu bilgi işlem birimlerinin bilişim güvenliği açısından istenen düzeye gelebilmeleri, kurum bilişim faaliyetlerini güvenli bir şekilde yürütebilmeleri ve güvenlik bilincinin artırılabilmesi için;

- Kamuda bilgi işlem birimlerinin yeniden yapılanması ve bilişim personeli görev ve unvanlarına ilişkin bir standardın oluşturulması,
- Güvenlik ile ilgili birim kurulması veya bu işleri yapacak bir personel görevlendirilmesi,
- Üst yönetimin desteğinin sağlanması,
- Uzman personele güvenlik eğitimleri sağlanması,
- Ağ güvenliğinin sağlanması,
- Erişim güvenliğinin sağlanması,
- Risk yönetiminin bulunması,
- Sistemlerin güvenlik açısından izlemesi,
- Önemli bilgilerin tasnifi ve etiketlenmesi,
- Tüm kullanıcılara güvenlik eğitimleri verilmesi,
- Kurumsal güvenlik politikası oluşturulması,
- Güvenlik uygulama talimatları hazırlanması,
- Fiziksel güvenliğin sağlanması

- Sistem test yöntemlerinin geliştirilmesi,
- Uygulamaların denetimi,
- Acil durum planlarının hazırlanması ve uygulanması gerekmektedir.

Güvenliğin çok pahalı bir sistem olduğu düşünülerek en önemli unsur olan güvenlik eğitimlerinin aksaksız uygulanarak kullanıcı bilinç düzeyi sürekli yükseltilmeli ve neyin güvenliğinin sağlanacağı sürekli sorgulanmalıdır. Çünkü bilişim sistemleri yaşayan ve gelişen sistemler olup durumları sürekli değişmektedir.

Etkin bir bilişim güvenliği ve genelde bilişim faaliyetlerinin başarısını sağlamak için gerekli görülen konular dünyadaki ve Türkiye deki örnekler araştırılmalı ve uygulanmalı, Bilgi İşlem birimleri kurumdaki en üst yöneticiye bağlanmalı ve kurumsal faaliyetlerin öncelikleri ve önemi en yetkili yönetici tarafından belirlenmeli, kamu bilgi işlem birimleri yeniden yapılanmalı görev ve sorumluluklar açık ve net olarak tanımlanmalı, kurumun güvenliği ve bilgi güvenliğinden sorumlu birimler atanmalı ve eşgüdümlü çalışmaları sağlanmalı, tüm personele güvenlik eğitimleri konumlarına uygun olarak verilmeli, Eğitimlerde süreklilik sağlanmalı, kurumun bilgi modeli ve hassasiyetleri ortaya çıkarılmalı, kurum güvenlik politika dokümanı hazırlanmalı ve bu dokümana göre tüm işlemler ödünsüz uygulanmalı, fiziksel ve elektronik güvenlik önlemleri bir bütün içinde belirlenmeli, bilişim sistemlerinin projelendirilmesinden, test, kabul ve işletilmesine kadar olan süreçlerde güvenlik ile ilgili riskler belirlenmeli, kontrol ve testleri yapılmalı, kullanıcıların yetki düzeyleri çok iyi belirlenmeli ve takibi yapılmalı, mümkünse yerli ürünler kullanılmalı, sistemler sürekli olarak güvenlik personeli tarafından izlenmeli, yedekleme ve acil durum planları hazırlanmalı, güvenlik açısından da önemli olan sistemlerin ve güvenlik gereçlerinin yerli yazılım ve teknolojilerle korunması için AR-GE çalışmaları desteklenmelidir.

Kamu Kurum ve Kuruluşlarının Bilgi İşlem merkezlerine uygulanan anketler sonucunda birçok kurumda aynı problemlerle karşılaşılmıştır, kurumlar sorunların çözümlerini kendi içlerinde ferdi olarak çözme yoluna gitmiştir, çözümü benzer

uygulama yapan kurumlardan destek alarak yapmalıdır.

Bilgi güvenliği politikaları öncelikle Bilgi İşlem merkezlerinden başlamalı, daha sonra tüm kuruma planlı olarak yaygınlaştırılmalıdır. Kamu bilgi İşlem yöneticileri konusunda uzman, bilgi birikimine sahip kişilerden seçilmeli, kurum üst yöneticileri bilgi teknolojileri konusunda bilinçlendirilmelidir. Bilgi teknolojilerine destekleri tam olarak sağlanmalıdır. Kurumun internet bant genişlikleri ihtiyaca göre seçilmeli, internet kullanıcıları bilinçlendirilmelidir. Eğitim yatırımları artırılmalı, eğitime daha çok ağırlık verilmelidir. Kurumları bilgisayar çöplüğü durumuna getirmeden, ihtiyaçları iyi belirlemeli, ihtiyaca göre alım yapılmalı, kurum bütçeleri optimum seviyede kullanılmalıdır. Donanım bakımları yapılırken, eski donanımlara yapılacak yatırımlarla yeni yapılacak yatırımlar arasındaki fark iyi analiz edilmeli, yapılacak yatırımlar doğru seçilmelidir.

Verilerin korunmasına önem verilmeli, kişisel verilerin korunmasında hak ve gizlilikleri ön planda tutulmalıdır. Felaketlerin oluşumu sonucunda, sistemlerin veya verilerin korunması ve hizmetlerin kesintisiz sağlanması bakımından her kurumun sistemlerinin bir yedeği başka bir kurum içinde veya başka bir bölgede (disaster recovery) bulunmalıdır. Felaket sonrası yazılı bir.güvenlik politikası belirlenmelidir. Güvenlik denetimleri periyodik olarak sürekli yapılmalı.

Kullanıcı şifreleri mümkün olduğunca alfanümerik ve uzun karakterlerden oluşturulmalı, sık sık değiştirilmelidir. Kamu kurumlarında ortak yazılımlar kullanılmalı, yazılımda Standard sağlanmalıdır. Kamuda E-imza kullanımı hızla yaygınlaştırılmalı, güvenli işlemlerin gerçekleştirilmesi sağlanmalıdır. Çalışanlara hukuksal hakları ve sorumlulukları anlatılmalı, hata yapmaları önlenmelidir.

Bilgi İşlem çalışanlarına belli standartlar getirilmeli, kurumlarda oluşan ve hatta aynı birimlerde oluşan hak kayıpları, farklı ücret politikaları ortadan kaldırılmalı, çalışma barışı sağlanmalı, Gelir politikaları düzgün belirlenmelidir.

Kamu kurum ve kuruluşlarda başarılı uygulamalar büyük bir fırsat olarak algılanmalı ve çözüm için çalışmalar birleştirilmelidir. Sorunların orta ve uzun vadede çözülebilmesi için gerekli girişimler de teknoloji gruplarıyla birlikte yürütülmelidir.

Sanayileşme sonrası, bilgi toplumu, yeni temel teknolojilerin gelişimiyle bilgi sektörünün, bilgi üretiminin, bilgi sermayesinin ve nitelikli insan faktörünün önem kazandığı bu yüzyılda bilgi güvenliği ön plana çıkmıştır. Bu nedenle kamu kurumları, bilgi güvenliği konusuna yatırımlarını artırmalı, yönetici ve çalışanlarını bilinçlendirmelidir. Kamuda birlikte çalışabilirlik desteklenmeli, bilgi paylaşımı maksimum seviyede tutulmalıdır.

KAYNAKLAR

1. 5070 sayılı Elektronik İmza Kanunu, 23 Ocak 2004 tarih ve 25355 sayılı resmi gazete, Ankara, (2004).

2. 2004/21 Sayılı, 06.09.2004 tarihli "Kamu Sertifikasyon Merkezi Oluşturulması" ***Başbakanlık genelgesi,*** Ankara, (2004).

3. Akçal, İ. T.C. "Kamu Kurumlarında Bilgi Yönetimi", ***Kültür ve Turizm Bakanlığı Milli Kütüphane Başkanlığı***, Ankara, 1, (2004).

4. Akman, K. İ. "E-devlet: Bilişim Güvenliği", ***Türkiye Bilişim derneği***, Ankara, 8, (2004).

5. Banfield, J. D. & Raftery, A. E. ***Modl-based Gaussian and non-Gaussian clustering. Biometrics,*** 49: 803-821, (1993).

6. Canbek, G. Sağıroğlu Ş. "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri", ***Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi,*** 23 (1-2):1-12, (2007).

7. Carlson, T. ISO 17799 Information Security Management: Understanding, CISSP, Lucent Technologies Worldwide Services, http://www.netbotz.com/library/ISO_17799.pdf, Ankara, 6, (2002).

8. Çağlayan, M. U. Bilgi Güvenliği: Dünyadaki Eğilimler, ***ULAKNET Sistem Yönetimi Konferansı-Güvenlik***, Ankara, 6, (2003).

9. Çetinkaya, M. "Kurumlarda Bilgi güvenliği Yönetim Sistemi'nin Uygulanması", Akademik Bilişim 2008, ***Çanakkale Onsekiz Mart Üniversitesi***, http://ab.org.tr/ab08/kitap/Bildiriler/139_152_AB08.pdf, Çanakkale, (2008).

10. Genç, H. "Açık Anahtar Altyapısı ve Problemleri", ***Gebze İleri teknoloji Enstitüsü***, Bilgisayar Mühendisliği, Kocaeli, (2003).

11. Güngören, B. "Bilgi güvenliği nedir?", ***TMMOB Elektrik Mühendisleri Odası, Ankara Şubesi Haber Bülteni,*** Ankara, 6-7, (2008).

12. http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/84200-bilgisayar-guvenligi.html.

13. http://www.izafet.com/güvenlik-ve–güvenlik-aciklar/8447-turkiyedeki-sirketlerde-gorulen-guvenlik-aciklari.html.

14. http: //www.izafet.com/güvenlik-ve–güvenlik-aciklar.

15. ISO/IEC 27001, Mart 2006, ICS 35.040 "Information technology–security techniques - Information security management systems – Requirements", ***Türk Standartları Enstitüsü***, Ankara, (2006).

16. ***Internet World Stats,*** "Useng and Population Statistics" http//www.internetworldstats.com/stats4.htm

17. Kumaş, E. "Kurumlar üstü bilgi güvenliği stratejisi", ***Türksat Uydu ve Kablo TV operatörü A.Ş. Bilgi Teknolojileri Direktörlüğü***, Ankara, (2009).

18. Kutsal, A. "***Türkiye İnternet Sektörü Raporu***", 16 mayıs 2008. http//webrazzi.com/2008/05/16/turkiye-internet-sektoru-raporu, Ankara, 1-6, (2008).

19. Krause, M. H.F. Tipton, "Handbook of Information Security Management", ***Auerbach Publications***, 6, 2007.

20. Melia, M. & Heckerman, D. An experimental comparison of several clustering and initialization methods, ***Microsoft Research Technical Report,*** MSR-TR-98-06, (1998).

21. Niğar, D. ve Yıldız, S, "Bilgi Yönetimi ve Örgütsel Etkinlik: Örgüt kültürü ve Örgüt Yapısının Temel İlkeleri", ***Abant İzzet Baysal Üniversitesi, Abant Üniversitesi, Ege Akademik Bakış,*** 10 (1):71-93 (2010)

22. Nazlı, M. ***Anadolubank A.Ş***.", Çevresel ve Fiziksel güvenlik" http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/fiziksel-ve-cevresel-guvenlik.html, (2010).

23. Nazlı, M. ***Anadolubank A.Ş.***, "Bilgi Güvenliği Açısından Haberleşme ve İletişim Yönetimi", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilgi-guvenligi-acisindan-haberlesme-ve-isletim-yonetimi.html, (2009).

24. Özgüler, C. V, "Verimlilik" ***Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi,*** Çalışma Ekonomisi ve Endüstri İlişkiler Fakültesi, http//www.yeniekonomi.com, (2008).

25. Öztürk, G. Bilgi Güvenliği Politikası oluşturma kılavuzu, ***Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü***, BGYS-0005. Kocaeli, 5-7, (2008).

26. Önel, D. ve Dinçkan A., "Bilgi güvenliği yönetim sistemi kurulumu", ***Ulusal Elektronik ve Kriptoloji Araştırma Enstitüs,*** (UEKAE), Ankara, 2, (2007).

27. ***Türkiye İstatistik Kurumu,*** "2009 Girişimlerde bilişim teknolojileri kullanım anketi" anket sonuçları, Ankara, (2009).

28. ***Türkiye Bilişim Derneği yayınları***", Saldırı Türleri ve Kurumlarda Görülen Açıklar", Ankara, 1-6, (2003).

29. ***Türkiye Bilişim Derneği yayınları***, "Bilişim sistemleri güvenliği el kitabı", Ankara, 1-7, (2006).

30. Vural, Y. Sağıroğlu, Ş. "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme", ***STM A.Ş.***, ***Bilgisayar Mühendisliği Bölümü, Mühendislik-Mimarlık Fakültesi, Gazi Üniversitesi***, Ankara, 2-4, (2008).

EKLER

EK-1. Anket Formu

KAMU BİLGİ İŞLEM MERKEZLERİNİN GÜVENLİK BAKIMINDAN İNCELENMESİNE YÖNELİK ANKET FORMU

Sayın ilgili;
Kamu kurum ve kuruluşları bilgi işlem merkezlerinin fiziki yapısını incelenmesi, donanım alt yapısının incelenmesi, veri-sistem güvenlik kalitesi bakımından durum tespiti ve bir güvenlik kalite sistem önerisi sunmak amacıyla, Gazi Üniversitesi istatistik Bölümü yüksek lisans tezi olarak bu çalışma yürütülmektedir. Bu çalışma sonucunda bilgi işlem merkezi yöneticileri ve teknik alt yapı sorumluları kendi bilgi işlem merkezlerini yeniden değerlendirme imkanı bulacaklardır. Bu nedenle, araştırmanın amaçlarının gerçekleşmesi, öncelikle sorulara vereceğiniz doğru cevaplara bağlıdır. Anket sorularının bu duyarlılıkla cevaplandırılması hususunda gerekli titizliğin gösterileceğinden şüphemiz yoktur.

Gizlilik
Vereceğiniz bilgiler, sadece istatistiksel çalışmalarda kullanılmak amacıyla toplanmakta olup, gizliliği teminat altına alınmıştır. Bilgiler herhangi bir mükellefiyetin doğmasında veya tahkikatın yapılmasında delil olarak kullanılmaz.

Yöntem ve Kapsam
Bu soru kağıdı, Kamu bilgi işlem merkezi yöneticileri yanında, kamuda çalışan teknik bilgiye sahip personele yöneltilecek sorulardan oluşmaktadır.

..../..../2009

A-1 **Bilgi işlem merkezinin idari yapısı nedir? (Yönetici cevaplandıracak)**

1 ☐ Bilgi işlem genel müdürlüğü

2 ☐ Bilgi işlem başkanlığı

3 ☐ Bilgi işlem daire başkanlığı

4 ☐ Bilgi işlem müdürlüğü

5 ☐ Bilgi işlem şube müdürlüğü

6 ☐ Bilgi işlem merkezi

7 ☐ Bilgi işlem Şefliği/Büro amirliği

8 ☐ Diğer:……

A-2 **Kurumunuzdaki aktif kullanıcı sayısı kaç kişidir? (ağa bağlı sistemde tanımlı uç sayıları)**

1 ☐ 0-50

2 ☐ 50-100

3 ☐ 100-500

4 ☐ 500-1000

5 ☐ 1000 - +

A-3 **Bilgi işlem merkezinde toplam çalışan personel sayısı kaç kişidir? (birim yöneticisi dahil çalışan sayısı)**

……

EK-1. (Devam) Anket Formu

A-4 **Bilgi işlem merkezinde çalışan personelin eğitim düzeyi nedir?(En son alınan diploma esas alınarak cevaplandırılacak)**

1 ☐ İlköğretim ..... kişi

2 ☐ Lise ..... kişi

3 ☐ Ön lisans ..... kişi

4 ☐ Lisans ..... kişi

5 ☐ Yüksek lisans..... kişi

6 ☐ Doktora..... kişi

A-5 **Kurumunuzda çalışan personele son 3 yıl içinde düzenli bilgisayar ve/veya bilgisayar güvenliği eğitimi verildi mi?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru B-8'e geçiniz

A-6 **Kurumda çalışan personele bilgisayar ve bilgisayarı güvenli kullanım eğitimi hangi sıklıkla verildi?**

1 ☐ Sıklıkla (yılda 3 ya da 4 defa)

2 ☐ Arasıra (yılda bir defa)

3 ☐ Nadiren (iki yılda bir defa)

4 ☐ Hiç verilmedi

5 ☐ Diğer:.....

A-7 **Ne tür eğitimler verilmektedir? (Birden çok seçenek işaretlenebilir)**

1 ☐ PC güvenliği konusunda bilgilendirme eğitimi

2 ☐ Bilgisayar temel eğitimi (İşletim sistemi,internet kullanımı, e-posta, vb.)

3 ☐ Ofis programları kullanımı eğitimi (Word, Excel, Powepoint vb.)

4 ☐ İleri düzeyde kullanıcı eğitimi (Local admin)

5 ☐ Teknisyenlik eğitimi

6 ☐ Diğer:.....

B-8 **Kurumunuzda kulanıcılara internet hizmeti veriliyor mu?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru B-13'e geçiniz

B-9 **Kurumunuzda ne tür internet bağlantısı kullanılıyor(Birden fazla seçenek işaretleyebilirsiniz)?**

1 ☐ Metro ethernet

2 ☐ ADSL

3 ☐ ISDN

4 ☐ Dial-Up

5 ☐ X25

6 ☐ Diğer:.....

EK-1. (Devam) Anket Formu

B-10 **İnternet çıkış hızınız kaç Mbps'dir?**

……

B-11 **İnternet hizmetinden tüm kurum personeli yararlandırılıyor mu?**

1 ☐ Evet 2 ☐ Hayır

B-12 **Kurumunuzdaki internet kullanıcılarından size gelen <u>en sık</u> sorunlar hangileri'dir? (en sık rastlanan üç sorunu işaretleyiniz)**

1 ☐ Virüs benim için zaman ya da bilgi kaybına neden oldu

2 ☐ Kredi kartı kullanımında usulsüzlük sebebiyle zarar gördüm

3 ☐ Kişisel bilgilerim internet üzerinden başkalarının eline geçti

4 ☐ Bana istemediğim iletilerin (e-posta) gönderilmesi (spam)

5 ☐ Diğer:……

6 ☐ Herhangi bir güvenlik sorunu yaşamadım

B-13 **Personelin internet üzerinden banka, fatura, vergi... v.b. işlemlerini yapmasında herhangi bir kısıtlama var mı?**

1 ☐ Evet 2 ☐ Hayır

B-14 **Biriminizde bilişim teknolojileri (BT) ile ilgili sürekli bir yayın takip ediliyor mu?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru C-16''ye geçin)

B-15 **Bilişim teknolojilerindeki güncel teknolojik gelişmeleri ne şekilde takip ediyorsunuz? (Sıklık sırasına göre, birden fazla seçenek işaretleyebilirsiniz)?**

1 ☐ İnternetten ilgili web sitelerinden

2 ☐ E-posta yolu ile

3 ☐ Dergi ve gazetelerden

4 ☐ Televizyonlardan

5 ☐ Toplantı ve seminerlerden

6 ☐ Diğer:……

C-16 **Bilgi İşlem merkezindeki sunucu sayısı (intel + unix v.s) kaç tanedir?**

……

C-17 **Kurumunuzdaki iletişimi sağlayan (Ana omurga, kenar switch vb.) aktif cihaz sayısı kaçtır?**

……

C-18 **Kurumda kullanılan masa üstü bilgisayar sayısı kaç tanedir?**

……

C-19 **Kurumda kullanılan dizüstü bilgisayar sayısı kaç tanedir?**

……

C-20 **Kurumda kullanılan yazıcı sayısı kaç tanedir?**

……

EK-1. (Devam) Anket Formu

C-21 **Kurumda kullanılan tarayıcı sayısı kaç tanedir?**

……

C-22 **Kurumun donanım bakımlarını yaparken/yaptırırken hangi yolu izliyorsunuz? (Son yılı dikkate alarak, birden fazla seçenek işaretleyebilirsiniz)?**

1 ☐ Bakımları kendi imkanlarımızla yapıyoruz

2 ☐ Arıza meydana geldikçe yetkili servislere çağrı açarak yaptırıyoruz

3 ☐ İhale ederek parçalı bakım sözleşmesi yapıyoruz

4 ☐ İhale ederek parçasız bakım sözleşmesi yapıyoruz

5 ☐ Diğer:……

C-23 **İş yeriniz size yeterli teknik (donanım/yazılım) imkanı sağlıyor mu?**

1 ☐ Evet

2 ☐ Hayır

3 ☐ Kısmen

C-24 **Kurumunuzda bilgi işlem merkezine ayrılan yıllık bütçe miktarı ne kadardır?**

…… TL.

C-25 **Bilgi işlem birimi için yıllık bakıma ayrılan bütçe miktarı ne kadardır?**

…… TL.

D-26 **Bilgi İşlem merkezinde Güvenlik yazılımı(Firewall) kullanılıyor mu?**

1 ☐ Evet 2 ☐ Hayır

D-27 **Güvenlik için ayrılmış bir donanımınız varmı?(güvenlik yazılımlarının üzerine kurulması için ayrılan cihaz)**

1 ☐ Evet 2 ☐ Hayır

D-28 **Antivirüs yazılımı kullanıyor musunuz?**

1 ☐ Evet 2 ☐ Hayır

D-29 **Birden fazla kullandığınız antivirüs yazılımınız var mı?**

1 ☐ Evet 2 ☐ Hayır

D-30 **Antivirüs ve işletim sistemi yazılımlarınızın güncellemeleri nasıl yapılmaktadır?**

1 ☐ Sistem merkezinden tek noktadan

2 ☐ Tüm kullanıcılara tek tek yüklenerek

3 ☐ Sunucular üzerinden paylaşılarak

4 ☐ Diğer:……

D-31 **Bilgilerinizin güvenliği için kriptolama kullanıyor musunuz?**

1 ☐ Evet 2 ☐ Hayır

EK-1. (Devam) Anket Formu

D-32 **Kurumun e-posta kullanımında öncelikle alınan güvenlik önlemleri nelerdir(Birden fazla seçenek işaretleyebilirsiniz)?**

1 ☐ Alfa nümerik e-posta şifreleri kullanmak

2 ☐ Güvenlik yazılımları kullanmak (e-posta, içerik filitrelemesi vb.)

3 ☐ Antivirüs yazılımı kullanmak

4 ☐ Diğer:……

D-33 **Veri tabanları için saldırı tespit sistemleri var mı(IPS)?**

1 ☐ Evet 2 ☐ Hayır

D-34 **Kurumunuz yazılı bir güvenlik politikasına dokümanına sahip midir?**

1 ☐ Evet 2 ☐ Hayır

D-35 **Kurumda sakıncalı siteler için filitreleme yapılıyor mu?**

1 ☐ Evet 2 ☐ Hayır

D-36 **Sisteminizdeki bilgilerin yedeğini alıyor musunuz?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru D-38'a geçin

D-37 **Hangi sıklıkla yedekleme alıyorsunuz?**

1 ☐ Her gün

2 ☐ Her hafta

3 ☐ Onbeş günde bir defa

4 ☐ Her ay

5 ☐ Altı ayda bir defa

6 ☐ Yılda bir defa

7 ☐ Diğer:……

D-38 **Sunucular üzerindeki veri tabanlarında kişisel bilgi tutuluyor mu?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru D-40'e geçin

D-39 **Kişisel bilgilerin güvenliği nasıl sağlanıyor. (birden fazla seçenek işaretleyebilirsiniz)?**

1 ☐ Firewall(güvenlik duvarı) ile

2 ☐ Erişimin şifrelerini sınırlandırarak (okuma, kayıt, silme vb.)

3 ☐ Verileri taşıma veya aktarım sırasında kriptolayarak

4 ☐ Uygulama sunucularına kontrolü erişim yetkisi ile

5 ☐ Diğer:……

D-40 **Kurumunuzda, bilgi işlem merkezindeki sistemlere saldırı tespiti ve izleme yapılıyor mu?**

1 ☐ Evet 2 ☐ Hayır

EK-1. (Devam) Anket Formu

D-41 **Bugüne kadar sisteminize saldırıda bulunuldu mu?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru D-44'e geçin

D-42 **Yapılan saldırı sonucu sisteminiz nasıl bir zarar gördü?(Birden çok seçenek işaretlenebilir)**

1 ☐ Web sayfası çalışmaz duruma getirildi

2 ☐ Sistemin tamamını çalışmaz duruma getirildi

3 ☐ Bilgileri kullanılmaz hale getirildi

4 ☐ Bilgiler tamamen veya kısmen veritabanından alındı/silindi

5 ☐ E-pota erişimi engellendi

6 ☐ Ağ erişimi engellendi

7 ☐ Veritabanı kullanılmaz hale getirildi

8 ☐ Verilerin içeriği değiştirildi

9 ☐ Herhangi bir zarar görmedi

D-43 **Verilen zararın maddi ya da manevi bakımdan hangisi daha ağırlıktadır?**

1 ☐ Maddi zarar daha ağırlıktaydı

2 ☐ Manevi zarar daha ağırlıktaydı(Prestij, güvenirlilik kayıbı vb.)

D-44 **Bilgi işlem merkezinde periyodik olarak güvenlik denetimi yapılıyor mu?**

1 ☐ Evet 2 ☐ Hayır

D-45 **Ağınızda alan (domain) yapısı varmı?**

1 ☐ Evet 2 ☐ Hayır

D-46 **Diğer kurum ve kuruluşlarla özel ağ bağlantınız var mı?(VPN)**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru D-48"e geçin

D-47 **Diğer kurum ve kuruluşlarla iki veya tek yönlü bilgi alış verişi yapılıyor mu?(VPN)**

1 ☐ Evet 2 ☐ Hayır

D-48 **Ağınızda Active directory yapısı var mı?**

1 ☐ Evet 2 ☐ Hayır

D-49 **Active directory yapısının sağladığı faydaları önem sırasına göre sıralayınız? (1'den 8'e kadar sıralayınız)**

1 ☐ Esnek sorgulama

2 ☐ Dizin hizmetleri ile birlikte çalışma yeteneği

3 ☐ DNS ile çalışabilirlik

4 ☐ Bilgi yenilenmesi

EK-1. (Devam) Anket Formu

5 ☐ Ölçeklenebilirlik

6 ☐ Genişletilebilirlik

7 ☐ İlkeye bağlı yönetim

8 ☐ Bilgi güvenliği

D-50 **Uç kullanıcılar sisteme hangi yöntemle dahil (login) oluyor?**

1 ☐ Kullanıcı şifreleri ile

2 ☐ Parmak izi kullanarak

3 ☐ Göz izi kullanarak

4 ☐ e-imza (token, kart vb) kullanarak

5 ☐ Şifreli kartlı sistemleri kullanarak

6 ☐ Diğer:……

D-51 **Bilgi işlem çalışanlarının sistem odasına giriş-çıkışları güvenlik bakımından hangi yöntemle sağlamaktadır. (birden fazla seçenek işaretleyebilirsiniz)?**

1 ☐ Kartlı sistemle

2 ☐ Göz izi kullanarak

3 ☐ Parmak izi kullanarak

4 ☐ Tuş takımı üzerinden şifre girerek

5 ☐ Diğer:……

D-52 **Sistem odası acil durum yönetimi için yazılı talimatınız var mı?**

1 ☐ Evet 2 ☐ Hayır

D-53 **Bilgi işlem merkezine giriş ve çıkışlar kurum çalışanlarına açık mı?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru D-55' geçin

D-54 **Bilgi işlem merkezine kurum çalışanlarının kapı geçiş güvenliği nasıl sağlanmaktadır?(Birden çok seçenek işaretleyebilirsiniz)**

1 ☐ Herhangi bir güvenlik önlemi yok

2 ☐ Kurum kartını göstererek

3 ☐ Özel giriş kartı alarak

4 ☐ İzine bağlı kimlik göstererek

5 ☐ Diğer:……

D-55 **Sistem odasında yangına karşı yangın söndürme güvenlik sisteminiz var mı?**

1 ☐ Evet 2 ☐ Hayır

D-56 **Binanın veya bilgi işlem merkezinin dış güvenliği sağlayan kamera sistemi var mıdır?**

1 ☐ Evet 2 ☐ Hayır

D-57 **Kurumunuzun uygulamakta olduğu bir yazılı güvenlik standardı var mı?**

EK-1. (Devam) Anket Formu

1 ☐ Evet 2 ☐ Hayır

D-58 **Sistemin bir yedeği (disaster recovery) başka bir coğrafi bölgede var mıdır?**

1 ☐ Evet 2 ☐ Hayır

D-59 **Bilği İşlem merkezine ait yazılı bir felaket senaryonuz var mı?**

1 ☐ Evet 2 ☐ Hayır

D-60 **Kullanıcıların bilgisayarlar üzerinde yetkileri hangi düzeydedir?(Birden fazla seçenek işaretleyebilirsiniz)**

1 ☐ Herhangi bir sınırlandırma yok

2 ☐ Sadece kendi işi ile sınırlandırılmış

3 ☐ Görev yetki çerçevesinde sınırlandırılmış

4 ☐ Sohbet ve haberleşme programlarına yasaklanmış

5 ☐ İnternete çıkışları sınırlandırılmış

E-61 **Bilgi işlem çalışanı olarak kurumdaki kullanıcılara teknik destek veriyormu sunuz?**

1 ☐ Evet 2 ☐ Hayır

E-62 **Kurumunuzda açık kaynak kodlu yazılımlar kullanılıyor mu?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru D-64'e geçin

E-63 **Kullandığınız açık kaynak kodlu yazılımlar nelerdir?(Birden fazla seçenek işaretlenebilir)**

1 ☐ Linux

2 ☐ Pardus

3 ☐ Open office

4 ☐ Diğer:.....

E-64 **Kurumunuzda ofis otomasyonu (elektronik ortamda evrak, döküman yönetim sistemi) kullanılıyor mu?**

1 ☐ Evet 2 ☐ Hayır

E-65 **Kurumunuzda vatandaşa yönelik e-devlet kapsamında uygulamanız var mı?**

1 ☐ Evet 2 ☐ Hayır

E-66 **Şu anda işlemlerinizde e-imza kullanıyor musunuz?**

1 ☐ Evet 2 ☐ Hayır ⟶ Hayır ise soru F-70'e geçin

E-67 **Kullandığınız e-imza uygulamanız hangi aşamadadır?**

1 ☐ Henüz proje aşamasında

2 ☐ Sadece alt yapısı hazır (Donanım, yazılım)

3 ☐ Sertifikaları aldık kullanıma başlamadık

4 ☐ Herşey hazır kullanmaya başlamadık

5 ☐ Herşey hazır kullanıyoruz

EK-1. (Devam) Anket Formu

E-68 **Kurum içi veya kurum dışı uygulamalarda e-imza uygulamanız var mı?**

1 ☐ Sadece kurum içi uygulamalarda kullanıyoruz

2 ☐ Sadece kurum dışı uygulamalarda kullanıyoruz

3 ☐ Her iki uygulamada'da kullanıyoruz

E-69 **E-imza için danışmanlık desteği aldınız mı?**

1 ☐ Evet 2 ☐ Hayır

F-70 **Üst düzey yöneticilerinizin bilişim teknolojilerine bakış açısı nedir?**

1 ☐ Bilgisayara uzak, eski teknolojileri tercih ediyor

2 ☐ Yeterli desteği veriyor

3 ☐ Destek veriyor fakat yeterli değil

4 ☐ Hiç destek vermiyor

F-71 **Sunucularda tutulan bilginin güvenli olduğuna inanıyor musunuz?**

1 ☐ Evet 2 ☐ Hayır

F-72 **Çalıştığınız birime mahsus hukuki sorumluluklarınızı biliyor musunuz?(5651 sayılı yasa vb)**

1 ☐ Evet 2 ☐ Hayır

F-73 **Bilgi İşlem biriminde çalışmaktan memnun musunuz?**

1 ☐ Evet 2 ☐ Hayır

F-74 **Bilgi işlem merkezinde çalışanların aldığı maaş sizce yeterli mi?**

1 ☐ Evet 2 ☐ Hayır

F-75 **Kısaca bilgi güvenliği konusundaki düşünceleriniz belirtiniz?**

.....

.....

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı ve Soyadı	**:** Adnan YILMAZ
Doğum tarihi	**:** 11.12.1964
Doğum yeri	**:** Gümüşhane-Şiran
Medeni Hali	**:** Evli – 2 çocuk
Telefon	**:** 0 (312).335 99 38
Faks	**:** 0 (312).416.11.81
e-mail	**:** adnan@yargitay.gov.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Lisans	Hacettepe Üniversitesi İstatistik Bölümü	1989
Lise	Ankara Mimar Sinan Lisesi	1984

İş Deneyimi

Yıl	**Yer**	**Görev**
1990-1991	Bağ-Kur Genel müdürlüğü	Veri Hazırlama ve Kontrol İşletmeni
1997-2004	Başbakanlık	Donanım ve Teknik Destek müdürü
2004–2010	Yargıtay	Bilgi İşlem Merkezinde Teknik Müdür,

Yabancı Dil

İngilizce

Yayınlar

YILMAZ, A. BAKIR, M.A. "Kamu kurumlarında Bilgi Güvenliğine Yönelik Bir Durum Tespiti" Orta Doğu Teknik Üniversitesi Bilgi güvenliği ve kriptoloji semineri, 2010.

Hobiler

Mesleki konularda araştırma yapmak ve ilgili yayınları okumak, seyehat etmek, kitap okumak, Kültürel amaçlı dergi çıkarmak, spor yapmak