ARAŞTIRMA

Geliş Tarihi: 14 Kasım 2022
Kabul Tarihi: 26 Aralık 2022

KURUMSAL MİMARİ GÜVENLİK REFERANS MİMARİ MODELLERİNİN İNCELENMESİ

Examination Of Enterprise Architecture Security Reference Architectural Model

DOI: 10.58307/kaytek.1203417

Sibel KARAKUŞ ÖZTÜRK[1] Doç. Dr. İhsan Tolga MEDENİ[2]
Prof. Dr. Tunç Durmuş MEDENİ[3] Doç. Dr. Mehmet Serdar GÜZEL[4]

Özet

Çalışmanın amacı; dünyadaki mevcut kurumsal referans güvenlik mimarilerine odaklı tespitte bulunmak ve çıkarımlar üzerinden öneriler sunmaktır. Bu çalışma, sürdürebilirlik açısından risk yönetimi yaklaşımlarının, kurumsal referans güvenlik mimarisi temeline dayandırmaktadır. BT' leri kullanımı ve internetin yaygınlaşması ile birlikte Türkiye' de dijital dönüşüme bağlı bilgi güvenliği araştırmalarına yönelik araştırmaların hız kazandığı görülmektedir. Bu çalışmada kurumsal mimari, güvenlik mimarisi, bilgi güvenliği ve farkındalığı üzerine değerlendirmede bulunulmuştur. Aynı zamanda, kurumsal mimari ve güvenlik mimarisi etkileşimine ait stratejik öneme yönelik vurgu yapılmaktadır. Teknolojik ilerlemelerin temelinde, süreç ve insan, kurumsal bilgi güvenliği odağına değerlendirmeler yer almaktadır. Dünyadaki kurumsal güvenlik mimarisi modelleri, kamu kurum ve kuruşları çerçevesinden incelenmiştir. Araştırma, nitel araştırma yönteminden faydalanılarak hazırlanmıştır. Çalışmaya dair veriler, son 5 yıla ait güncel akademik tez ve makaleleri içeren literatür taramasını, ülkelere ait kurumsal web sayfası raporlarını ele alarak derlenmiştir. Kurumsal hizmet anlayışı alanında, bilgi güvenliğine yönelik risklerin strateji ve politikalarla güvence altına alınması gerektiği çıkarımı elde edilmiştir. Son olarak, kurumsal güvenlik mimarisi çerçeve uygulamaları, yetişmiş insan gücü, bireysel ve toplumsal eğitimlerle güvenlik farkındalığı yaratılarak tehditlerin önüne geçilebileceği sonuç tespitine ulaşılabilmektedir.

Anahtar Kelimeler: *Information security, enterprise architecture, e-service, digital transformation.*

Abstract

The aim of the study; to determine the existing corporate architectures in the world and to offer suggestions based on inferences. This study bases risk management approaches on sustainability on the basis of enterprise reference security architecture. With the use of IT and the widespread use of the internet, it is seen that researches on information security related to digital transformation have gained momentum in Turkey. In this study, an evaluation was made on corporate architecture, security architecture, information security and awareness. At the same time, emphasis is placed on the strategic importance of the interaction of enterprise architecture and security architecture. Process and human, corporate information security focus is on the basis of technological advances. The corporate security architecture models in the world have been examined from the perspective of public institutions and organizations. The research was prepared by using the qualitative research method. The data of the study were compiled by considering the literature review including the current academic theses and articles of the last 5 years, and the institutional web page reports of the countries. In the field of corporate service understanding, it was concluded that the risks related to information security should be secured with strategies and policies. Finally, it is possible to reach the conclusion that threats can be prevented by creating security awareness through corporate security architecture framework applications, trained manpower, and individual and social trainings.

Keywords: *Information security, enterprise architecture, e-service, digital transformation.*

[1]Sibel KARAKUŞ ÖZTÜRK, Yüksek Lisans Öğrencisi, ANKARA Yıldırım Beyazıt Üniversitesi, Yönetim Bilişim Sistemleri E-Devlet ve Kamuda Dönüşüm, sibelkarakus@hacettepe.edu.tr Orcid 0000-0002-4287-537X
[2]Doç. Dr. İhsan Tolga MEDENİ, ANKARA Yıldırım Beyazıt Üniversitesi, İşletme Fakültesi Yönetim Bilişim Sistemleri, tolgamedeni@ybu.edu.tr Orcid: 0000-0002-0642-7908
[3]Prof. Dr. Tunç Durmuş MEDENİ, ANKARA Yıldırım Beyazıt Üniversitesi, İşletme Fakültesi Yönetim Bilişim Sistemleri, tuncmedeni@ybu.edu.tr Orcid: 0000-0002-2964-3320
[4]Doç. Dr. Mehmet Serdar GÜZEL, ANKARA Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği mguzel@ankara.edu.tr Orcid: 0000-0002-3408-0083

1. GİRİŞ

Bilginin dijital ortama aktarılmasında yaşanan teknolojik ilerlemeler ve yaygın internet kullanımı, bilgiyi daha önemli bir noktaya getirmiştir. Kurumsal mimari yapısı, istikrarlı güvenlik mimarisi yaklaşımları ile hedef kitleyi, bilgi güvencesiyle risklerden arındırmaktadır. Kurumların ihtiyaç duyduğu bilgi güvencesi, kurumsal güvenlik mimarisi aracılığı ile sağlanmaktadır. Bu çalışma ile sadeleştirilmiş sürdürülebilir ve güvenli bir kurumsal mimariye olan ihtiyaç vurgulanmaktadır. Referans güvenlik çerçeve mimarileri, iş stratejileri, süreçleri, bilgi sistemleri dönüşümü, veri güvenliği ve altyapısını kapsamlı bir biçimde ele almaktadır. Kamu kurum ve kuruluşları e-hizmet dinamiklerini geliştirmek istediklerinde, araştırma kapsamındaki incelenmiş olunan kurumsal güvenlik mimari örneklerinden ihtiyaçları ölçüsünde faydalanabilme imkânı bulabileceklerdir. Bilgi güvenliğine yönelik riskler güvenlik mimarisine yönelik ihtiyacı ortaya çıkarmaktadır. Güvenlik mimarisi kurumsal mimarinin bütün bilişsel ve fiziksel boyutlarını ele almaktadır. Dijitalleşmenin bir sonucu olarak kurumsal güvenlik mimarisinin önemi günden güne artmaktadır. Yürütülmekte olan kurumsal mimari çalışmalarına entegre güvenlik mimarisi çerçevelerinin gerekliliği üzerine vurguda bulunulmuştur. Araştırma ile güvenlik mimarisine yönelik bütüncül bir çerçeve politikası ortaya koymaya yönelik değerlendirmede bulunulmaya çalışılmıştır. Çıkarımda bulunulmaya çalışılmıştır. Kurumsal mimari yapısı bütüncül olarak değerlendirildiğinde güvenlik bütün katmanlarda ele alınmaktadır. Kurumsal yapılanma, temelde, işleyiş, süreklilik, altyapıyı, teknoloji ve güvenlik unsurları açısından perspektif bir bakış açısı sunmaktadır. Bütüncül bir yaklaşım ile kurumsal güvenliğin temelleri kuvvetlendirilmektedir. Globalleşen dünyada üstünlük mücadelesi veren ülkeler yönünden bilgi önemli bir yere sahiptir. Dijital dünyada rekabet edebilmek için, bilgi güvenliği standart ve modellemelerinin, gereksinimler doğrultusunda hazırlanarak güncel tutulması gerekmektedir. İş, veri, uygulama ve altyapı mimarileri stratejik hedefleri oluşturulmaktadır. Bu doğrultuda en etkin risk yönetimi politikaları hazırlanmaya çalışılmaktadır. Strateji oluşturma ve risk yönetimi politikaları, süreç yönetiminde güvenlik mimarisini etkilemektedir. Kurumsallaşmanın önemi arttıkça, kurumsal mimariye yönelik daha fazla çalışma yürütülmeye başlanmıştır. Kurumsal mimari güvenlik referans çerçeve politikalarla desteklenmektedir. Kurumsal güvenlik mimari çerçevesi, kurum kültürüne uygun olarak yalın ve doğru ifadelerle tasvir edilmektedir. Yasal mevzuatlar çerçevesinde strateji oluşturulmaktadır. Kurumlar arası iletişim ile sorunlar anlık olarak paylaşılıp ortak çözüm önerileri geliştirilmeye çalışılmaktadır. Keşif haritası, ihtiyaç duyulan güvenlik mimarisine giden yolda avantajlar sunmaktadır. Güvenlik referans mimarisinin, kurumsal mimari altyapısı doğrultusunda ihtiyaçları güncellenerek birlikte çalışabilirliği denetlenebilmektedir. Kurumsal referans mimari süreç politikaları ile güvenliği ön planda tutmaktadır. Geleneksel güvenlik anlayışının kabukları kırılarak yeni teknoloji çağının meyvesi olan siber dünyanın ayak sesleri

yankılanmaktadır. Siber dünyada güvenlik tek taraflı olarak ele alınmamaktadır. Hizmet odaklı sunulan çalışmaların devamlılığı adına veri güvenliği önem arz etmektedir. Siber dünyada güvenlik açıkları, kamu kurumları üzerinde ek maliyetlere yol açabilmektedir. Kurumsal yapılanma üzerinde, bilinçli ve sağlam temellere dayandırılan bir güvenlik anlayışı hâkimiyeti kurulması üzerine vurgu yapılmaktadır.

Kurumsal güvenlik mimarilerine yönelik boşluklar, en doğru uygulanabilir süreç yönetimi, BT altyapısı, yetişmiş insan gücü ve farkındalık eğitimleriyle aşılabileceği gözler önüne serilmektedir. Bu amaçla tutarlı, şeffaf ve hesap verebilir güvenlik mimari yapısı örneği ortaya konulmaya çalışılmıştır. (Ayşe Bilge İnce, 2016)

Bilgi teknolojisindeki gelişmelere bağlı olarak siber âlem ile yeni bir dünyanın kapıları aralanmıştır. Dijital dünyanın sağlamış olduğu imkânlar gündelik yaşantımızı da etki etkilemektedir. Bilgi teknolojisindeki ilerlemelere bağlı olarak geleneksel kalıplar kırılmış ve bilişim teknolojisi devrimi gerçekleşmiştir. Kurumsal yapılanma içerisindeki kuruluşların, iş süreçleri içerisindeki, birimler arası sorumluluklarının sınırlarını, güvenlik açısından, belirlenmesi gerekmektedir. BT' leri alanındaki ilerlemeler, dokümanlara ait kayıtların fiziki bir ortamdan alınarak elektronik bir ortama aktarılması ile kurumsal açıdan e-belge güvenliğinin önemi artmıştır. Kurumsal güvenlik mimarisine yönelik çalışmaların küresel boyutlarda ele alınarak geliştirilmesi gerekmektedir. Hali hazırda kullanılmakta olan sistemlere ait yapısal ve teknik problemlerin çözüme kavuşturulması önem arz etmektedir. Covid -19 salgını ile birlikte, dünya devletleri birçok alanda olduğu gibi güvenlik konusunda da ciddi problemlerle karşı karşıya kalmıştır. Kurumsal yapılanmanın sahip olduğu güç, en zayıf domino taşı etkisi boyutundadır. Bilgi güvenliğine yönelik en ufak bir açık, bütün sistemin çökertilebilmesine yetebilmektedir. Güncel ve yenilenebilir teknoloji, personel farkındalığı, yetişmiş insan gücü, düzenli süreç yönetimi ve analizler ile güvenlik tedbirleri desteklenebilmektedir.

Bu çalışma ile kurumların teknoloji döngüsü içerisinde ne derece güvende olduklarına yönelik çıkarımda bulunulmaya çalışılmıştır. Bu noktada ülkelerin güvenlik mimari çerçeveleri incelenmiştir.

Ayrıca bu çalışma ile bilgi güvenliği ve kurumsal güvenlik mimarisi çalışmalarına yöneliktir.

Hedef kitleyi risklerden arındırmak, sürdürülebilirlik ve güvenlik mimarisinin olgunlaştırılmasına yönelik olarak bu çalışma 2. bölüm ile kurumsal mimari ve güvenlik mimarisi gelişimi detaylandırılırken, 3. bölüm ile de tarihsel ilerlemelere yer verilmiştir. Kurumsal mimari alt dalları ise 4. bölüm de detaylandırılmıştır. Güvenlik mimarisi hedefleri ve dünyada kurumsal mimari çalışmalar ise diğer bölümlerde anlatılmıştır.

2. KURUMSAL MİMARİ VE GÜVENLİK MİMARİSİ GELİŞİMİ

Kamusal hizmetlerin, iş süreçleri içerisindeki bilgi yoğunluğunun artması, BT' leri kullanımını artırmıştır. Zamanın ruhuna adapte e-devlet uygulamaları ve dijital dönüşüm çalışmaları blockzincir teknolojisi ile desteklenmektedir. Dijital dönüşümde elde edilen kazanımların temelini AR-GE faaliyetleri oluşturmaktadır. Mevcut kaynaklar ve tehditler değerlendirilerek yenilenen teknolojiye fırsat verilmesi gerekmektedir. Kurumsal güvenlik mimarisi kamusal hizmetlerin sorunsuz bir biçimde yürütülmesi için lokomotif görevini üstlenmektedir. Hızlı, verimli, düşük maliyetle güvenlik sağlanmaya çalışılmaktadır. Güçlü bir kurumsal güvenlik mimari nezdinde sınırlı sayıda çalışma yürütülebilmektedir. Referans mimari çakışmaları ile kamusal idarelere, teknik ve stratejik açılardan güvenli bir ortam sunulmaya çalışılmaktadır. Dijital dönüşüm ile bilgi akışı sınırları genişlemiş, bilgi güvenliği üzerinde titizlikle çalışılması gereken bir durum haline gelmiştir. Özel sektörde güvenlik mimarisi üzerine ciddi çalışmalar yürütülmekte iken, kamu kurumları mimari alt yapısı ise devlet destekli güvenlik temelleriyle desteklenmektedir. Kurumsal güvenliği geliştirmek adına;

- Ortak platformlar oluşturularak koordineli hareket teşvik edilmeli,
- Standartlar belirlenmeli,
- Kolay ve güvenli erişim için uygun altyapı oluşturulmalı,
- Risk yönetimi stratejisi belirlemede kaynak israfının önüne geçilmeli,
- Güvenlik yapılanmasına ait fonksiyonların sürdürülebilir kalkınma planı uyumuna dikkat edilmeli,

Geleneksel devletin hizmet anlayışında birçok bürokrasi aşaması bulunmaktadır. Yenilikçi e- devlet anlayışında ve de gelinen süreçte dijital devlet bakışıyla bürokrasi engeli, bilgi sistemleri aracılığı ile ortadan kalmaktadır. İnternet ve BT' leri aracılığı ile zamandan ve mekândan bağımsız olarak devlet ve özel sektör hizmetleri vatandaş ile sanal ortamda buluşmaktadır. Dijitalleşme ile merkezi ve yerel yönetimlere ait kurumsal hizmetlerin, devlet-vatandaş etkileşimi açısından çevrimiçi sunulması dinamik veri paylaşımı avantajı sunmaktadır. Kişisel ve kurumsal verilerin, e devlet uygulamaları ile desteklenmesi, bilgiyi resmi bir kimliğe kavuşturmuştur. Kurumsal hizmet kültürü yapılanması içerisinde kaynak yönetimi ve bilgi güvenliği altyapısının kurum içi ve dışı mevzuatlarla uyumlu olması gerekmektedir. Kamu bilgi sistemlerine ait çevrim içi e-kanalların iş süreçleri modellemeleri ve yönetimi içerisindeki etkinliği performans yönetimi açısından kritik öneme sahiptir.

Devletlerin küresel boyutta rekabet avantajı sağlayabilmesi için kurumsal hizmetlere yönelik ortak bir kurumsal mimari çerçevesi geliştirilmesi gerekmektedir. Kurumsal yapılanma içerisinde sunulan dijital hizmetlerin kalitesini artırmaya ve denetlemeye

yönelik olarak kapsamlı bir güvenlik mimarisi çerçevesinin kurumsal mimari içerisine dâhil edilmesi gerekliliği kaçınılmazdır. Kurumsal mimari, kullanıcıların toplumsal ve mali menfaatlerini gözetmek zorundadır. (ŞEN F, 2018)

Kurumsal güvenlik hedeflerinin, sürdürebilir iş hedefleri ile dengeye getirilmesi, tehditlere yönelik farkındalığın olgunlaşmasında etkin rol oynamaktadır. Kurumsal güvenlik mimarisi, kurumsal faaliyet alanına yönelik BT' leri tehditleri karşısında güvenlik algısı oluşturmaktadır. Güvenlik mimarisi yaklaşımı ile kurumsal hedefler, risk yönetimi konusunda dengeye getirilmeye çalışılmaktadır. Tehditler tamamen ortadan kaldırılmaya çalışılmakta, bu mümkün değil ise makul seviyede tutulmaya çalışılmaktadır. Riskler karmaşasında, sürdürebilir iş hedefleri, artırılmış farkındalık eğitimleri ve güvenlik operasyonlarının üst düzeyde tutulması ile BT' leri uygulamaları güvende tutmaktadır. Üst düzey güvenlik tedbirleri oluşturulurken, personel üzerinde aşırı müdahaleci bir yapı oluşturulması çalışanları kurumsal yapılanma içerisinde yeni güvenlik açıklarına yönlendirmektedir. Yüksek denetimli yapı çalışanları bu denetimli yapının yeni açıklarına bulmaya itmektedir. (Ritchot B, 2013)

Kurumsal mimari referans hizmetlerin pek çok avantajları bulunmaktadır. Bunlara örnek verecek olursak, kamusal hizmetler çevrimiçi olarak kesintisiz bir şekilde sunulmakta, şeffaflık sağlanmakta, tekrar eden ve hatalı verilerin önüne geçilmekte, coğrafi şartların elverişsiz olduğu durumlarda etkin hizmet anlayışı ile hizmetler sunulmakta, kamusal hizmet maliyetleri azalmaktadır. Kurumsal mimarinin sağlamış olduğu avantajlar güvenlik, iş, veri, uygulama ve teknoloji alt yapı faaliyetleri çatısı altında şekillenmektedir. Güvenlik mimarisi sınırları, veri güvenliğine yönelik olarak gerçekleşebilecek riskler ölçüsünde esnetilebilmektedir. Dijital dünyanın güvenliği farklı bir boyutta soyutlanarak ele alınmaktadır. Kurumsal mimari modelleme dili hazırlanırken, güvenlik mimarisine ait gereksinimler ve riskler kapsamlı bir şekilde ele alınmalıdır. Referans mimari modellemeleri aracılığı ile benzer güvenlik problemlerine yönelik ortak çözümler geliştirilebilmektedir. Güvenlik mimarisine ait mükemmel bir strateji bulunmamaktadır. İstenmeyen ve ani gerçekleşen bazı durumlar güvenlik mimarisi üzerinde domino etkisi yaratabilmektedir. Bazen de Nasrettin Hoca'nın mezarı gibi kapıyı kilitleriz ama diğer her yer açıktır. Bu yüzdendir ki güvenlik tek boyutta ele alınmamalı perspektif bir bakış açısıyla bütüncül bir biçimde ele alınmalıdır. Kamu kurum ve kuruluşları vermiş oldukları hizmetin doğası gereği, güvenliğe ait yetki sınırlarını mevzuata uygun bir biçimde strateji planı olarak belirlemelidir.

Güvenlik mimarisi, güvenlik adaptasyon ve maliyetlerin azaltılması stratejisi için bütüncül bir yaklaşım ile verimliliği sağlanmayı hedeflemektedir. Güvenliğin evrensel bir organizasyon yapısı bulunmamaktadır. Fakat güvenliğe yönelik bazı genel genelleşmiş ortak gereksinimler bulunmaktadır. İhtiyaçlar şekillendikçe gereksinimler belirgin hâle gelmektedir. Güvenlik sonradan düşünülecek bir yama değildir. Kurumsal mimari

çalışmaları ile eş zamanlı olarak geliştirilmesi gerekmektedir. Güvenlik çalışmalarına yönelik faaliyetler çözüm odaklı aktif pratiklerle ve stratejilerle desteklenmektedir. Mevzuat, yönerge ve strateji planlarıyla süreç ve yetkilendirme mekanizması sınırlandırılabilmektedir. Gelişen küresel dünyada rekabet edebilmek ve veri kayıplarının önüne geçebilmek için güvenliği kurumsal mimari maliyetleri içerisinde değerlendirmek gerekmektedir.

3. KURUMSAL MİMARİ ve GÜVENLİK MİMARİSİ TARİHSEL İLERLEMELERİ

Kurum; bir amaca yönelik olarak oluşturulan özel veya devlete ait olan kuruluştur. (TÜRKKAHRAMAN, P. D. M, 2004)

Kurumsal yönetim, işin gerektirdiği ahlaki etik kurallarla çevrili, şeffaf ve hesap verebilir nitelikte olmalıdır. Ayrıca veri güvenliğine yönelik tehditlere karşı denetim mekanizmasının bütüncül bir yapıya sahip olması gerekmektedir. Kurumsal hizmet yönetiminde yeterli olgunluk ve güvenlik düzeyine erişilmesi maddi ve itibari açıdan pek çok avantajlar sunmaktadır.

Kurumsal mimari; ortak politikalar ve standartlarla teknoloji altyapısına uyarlanarak, sistem içerisindeki bütünlüğü, etkinliği ve verimliliği kurumsal hedefler doğrultusunda sağlamaktır. Kurumsal hiyerarşi kademelendirilerek geçmiş ve gelecek arasında köprü kurulup stratejik hedefler belirlenmektedir. Mevcuttaki durum ileri teknoloji ile değerlendirilerek uygun bir uygulama planı oluşturulmaya çalışılmaktadır.

Kurumsal mimari, hizmet işleyişi üzerinde aktif bir biçimde belirleyici bir rol almaktadır. Tekrar eden süreç döngüsüne ait ortak uygulamaların ardışık faaliyetlerine son vermektedir. Ortak platformlar aracılığı ile koordinasyon sağlanmaktadır. BT' leri alanındaki ilerlemelerin kurumsal hizmet anlayışı üzerinde olumlu etkisi bulunmaktadır. (Menteşe, Özbilgin, Arslan, 2017).

Kurumsal mimari, John Zachman tarafından 1987 tarihinde evrene yayılmıştır. Dr. Steven H. Spewak 1992 yılında hazırlamış olduğu 'Enterprise Architecture Planning' yayın ile ilk defa kurumsal mimari teriminin altı çizmiştir. Kurumsal mimariyi yaklaşım olarak benimseyen TAFIM (Technical Framework for Information Management)' dır. 1995 yılında TOGAF(The Open Group Architecture) TAFIM' dan etkilenilerek geliştirilmiştir. FEAF (Federal Enterprise Architecture Framework) 1999 yılında ABD tarafından iş, teknoloji ve strateji hedeflerini geliştirmeye yönelik olarak hazırlandı. 2005 yılında MODAF (Ministry of Architecture Framework) Birleşik Krallık ve 2007 yılında DNDAF (Department of National Defences) Kanada bünyesinde geliştirilmişlerdir. Kurumsal mimariye ait çalışmalar 1987 yılından bugüne kadar gelmesine karşılık hala arzulanan hedefe ulaşılamamıştır (GÜMÜŞ, 2018).

Güvenlik mimarisi, iş süreçlerinin ve risk analizlerinin en verimli şekilde değerlendirilmesidir. 1995' ten beri güvenlik mimarisi terimi araştırmacıların gündemindedir. Güvenlik mimarisi kurumsal hiyerarşi içerisinde dijital olgunluk düzeyini artırmaktadır. Kamu kurumlarında düzeli işleyen bir denetim mekanizması, güncel teknoloji ve bütüncül bakış açısı ile süreçler en iyi şekilde yönetilebilmektedir. Yazılım ve donanım açısından ortak bir dil kullanılması ve ortak bir güvenlik kültürü çerçevesinde hareket, tehditler karşısında kalkan görevi üstlenmektedir. (BAŞARANOĞLU, E. 11/05/2020).

4. KURUMSAL MİMARİ ALT DALLARI

Kurumsal mimari, kurumsal bir yapıyı bütünsel bir biçimde ele almaktadır. Ortak dil kullanımı paydaşlar arasında işbirliğini desteklemektedir. Farklı bakış açıları, farklı paydaşlar mevcut ve hedeflenen durumlar karşısında avantaj sağlayabilmektedir. Kurumsal yapılanma standart ve politikalar aracılığı ile kurumsal misyon gerçekleştirmeye çalışmaktadır. Sistem tasarımına yönelik işlevsel yapı özellikleri sınırları oluşturulmaya çalışılmaktadır. Standart ve politikalar bu yönüyle birbirleriyle bağlantılıdır. (Sara Larno, V.S and J. Nurmi, 2019)

Kurumsal mimarinin, mevcut ve ileriye dönük hedeflenene ulaşması iş süreçlerine, iş sürekliliğine ve BİT' lerine bağlıdır. Birçok mimari sürdürülebilirliği çoğu zaman göz ardı etmektedir. Birçok kurumsal mimari yapısı bulunmasına karşılık literatürde ki mimariler güvenlik ve sürdürebilirlik üzerinde yoğunlaşmamaktadırlar. (Rahman, M. T. U. A. N. I. B. M. M, 2017)

Kurumsal mimari yapısı;

- İş Mimarisi
- Veri Mimarisi
- Uygulama Mimarisi
- Altyapı Mimarisi

Güvenlik Mimarisi katmanlarından oluşmaktadır.

4.1. İş Mimarisi

Kurumsal yapı nezdinde iş mimarisi, birimler arası iletişim ve ortak hareket ile işin faaliyet hedeflerinin gerçekleştirilmesidir. İş mimarisi, iş yeteneklerini adreslemiş olduğumuz bölümü oluşturmaktadır. Kurumsal yapı içerisinde yürütülmekte olan bütün değerleme basamaklarını bünyesinde barındırmaktadır.

Hızlı hizmet sunumu ve kolay erişim ile e -hizmetler bütüncül olarak iş mimarisiyle ilişkilendirilmektedir. Kurumsal iş stratejisi ve organizasyonları kurumsal hedeflere

ulaşmak için basamak oluşturmaktadır. Hedefler ve gereksinimler doğrultusunda iş mimarisi geliştirilebilmektedir. (Rahman, M. T. U. A. N. I. B. M. M, 2017)

İş planlaması, iş süreçlerinin olgunlaşması ve yürütülmesinde etken bir rol almaktadır. Çerçeve protokollerle, kurumsal faaliyetlere yönelik yaklaşımlar bütünlük kazanmaktadır. Sistemsel hayat skalası, işleyiş yapısına ait özelliklerden ve süreçlerden oluşmaktadır. İş mimarisi faaliyetlerinin yürütülmesinde karşı karşıya kalınan risklerle başa çıkmanın en etkili yolu, güvenlik mimarisi temellerini kurumsal yapı bünyesinde barındırmaktır. İş süreçlerin yeni nesil teknoloji ile iyileştirilmesi iki aşamada gerçekleşmektedir.

a) Basitleştirilmesi (Basit ifade edilmesi, yalın hale getirilmesi)

b) Doğru tanımlanması gerekmektedir. (Jeganathan S, 2017)

4.2. Veri Mimarisi

Veri sınıflandırması ve erişim yetkilendirmesi konusunda belirleyici çözüm önerileri sunmaktadır. Veriye ait mantıksal modellemelerinin, standartların ve yaşam döngüsünün belirlendiği bölümdür. Teknolojik ilerlemelerin çok hızlı gelişmesi ve etkilerinin çok büyük olması, proje yönetimini derinden etkilemektedir. Sistemler arası etkileşimlerin fazla olması parçaların yönetme konusunda bir karmaşıklığa neden olabilmektedir. Kurumsal mimari değişim hızının fazla olması yenilikçi bir yapıya sahip olduğunun bir göstergesidir. Referans mimari belirsizlik ve karmaşıklığın yaşandığı noktada, kurumsal yapıyı bir bütün olarak ele almakta ve hedeflere ulaşma konusunda bizlere aksiyonları sunmaktadır. Bilginin derlenmesi, işlenmesi, sınıflandırılması ve paylaşılması aşamalarını içermektedir.

4.3. Uygulama Mimarisi

Kurumsal hizmet anlayışı içerisinde sunulmakta olan uygulamaların portföyünü oluşturmaktadır. Uygulamada olan ve test aşamasındaki hizmet odaklı uygulamaların, portföy içerisindeki yerleri hakkında değerlendirmede bulunulmaktadır. Kurumsal yapılanmaya ait iş süreçleri, gelişen teknolojiye uygun olarak yenilenmektedir. Kurumsal mimari alt yapısında kullanılmakta olan uygulamaların da eş zamanlı olarak güncellenmesi gerekmektedir. Kurumsal e-hizmetlere yönelik işlevsellik kazandırılarak yetkisiz erişimin önüne geçmeye çalışılmaktadır. Güncel teknolojiden faydalanılarak log yönetimi ve izleme sistemi aracılığı ile bilgiler üzerinde denetim sağlanmaktadır. Yazılım ve donanım tabanlı olarak güvenlik çerçeve mimarisi tasarlanmaya çalışılmaktadır. (Wahe, I. U. M. A. S. A. W. A, 2017)

4.4. Altyapı Mimarisi

Kurumsal hizmetlerin gerçekleştirilmesinde kullanılan yazılım ve donanım alt yapısının teknoloji temeline dayandırılmasıdır. Uygulama mimarisinin, veri tabanındaki politikaları üzerinde düzenlemede bulunulmaktadır. Ortak çözüm yolları üretilerek riskler

ortadan kaldırılabilmektedir. Kurumsal hizmetlerde yaşanan aksaklıklar farkındalık eksikliğinden veya teknik problemlerden kaynaklı olarak gerçekleşebilmektedir. Kurumsal hizmet uygulamalarının güvenliğine ve kişisel verin korunmasına yönelik olarak uygulama alt yapısı sürekli olarak dinamik tutulmaktadır. (Çözümleri, H. B, 2015).

4.5. Güvenlik Mimarisi

Kurumsal hizmetler yürütülür iken bilgi güvenliği unsurları gözetilerek, ihtiyaçlar belirlenmektedir. Sürdürülebilir bir kurumsal mimari için oklar güvenlik mimarisini işaret etmektedir. Güvenlik çerçeve yaklaşımı kurumsal mimari katmanlarının sorunsuz bir biçimde işleyişini sağlamaktadır. Güvenlik kontrollerinin, kişisel verileri korumaya ve veri mahremiyetini sağlamaya yönelik olarak gerçekleştirilmesi gerekmektedir. Teknolojinin yer aldığı her alanda güvenliğe yer verilmelidir. Alanında yetişmiş eğitimli kişilerle tehditler karşısında veri bütünlüğü sağlanmaya çalışılmaktadır. (İLHAN, E. and Ö. F. YELKENCİ , 2021)

Kurumsal güvenlik risk yönetimi kritik alt yapı uygulamaları üzerinde etkilidir. Mevcut kurumsal mimari güvenlik mimarisiyle bütünsel bir biçimde entegredir. (Nather S, 2018)

Kurumsal hizmetler çeşitlendikçe kişiler ve kurumlara ait veri oranlarında artış olmaktadır. Mevcut güvenlik tedbirleri bu artışlar karşısında zamanla yetersiz kalmaktadır. Kritik alt yapıları korumaya yönelik olarak siber saldırılara karşı duyarlı küresel boyutta bir güvenlik mimarisine ihtiyaç duyulmaktadır. (ÇİFTÇİ E, 2021)

Kurumsal hizmet yönetimi blockchain uygulaması ile veri paylaşımı içerisinde güvenliği üst düzeyde tutmak zorundadır. Belirli aralıklarla gerçekleştirilen güvenlik taramaları ve donanım bakım onarım çalışmaları ile güvenlik zaafiyetlerinin önüne geçilebilmektedir. (KAYA, Ö. F, 2017)

5. BİLGİ GÜVENLİĞİ

İnsan beyninin yorumlayabildiği hakikatler bilgiyi ifade etmektedir. Verinin bütünleşerek bir anlam kazanması onu bilgiye dönüştürmektedir. İnternet ve BT' leri aracılığı ile kişisel ve kurumsal veriler işlenmektedir. İşlenen veriler bilişim sistemleri bünyesinde ki kurumsal hizmetler bandında yer almaktadır. Gizlilik, bütünlük ve erişilebilirlik bilgi güvenliği unsurlarındandır. Bilgi güvenliğine yönelik standartlar ve sertifikalar geliştirilerek verilerin bütünlüğü korunmaya çalışılmaktadır. Tek boyutlu olarak güvenliğin sağlanmaya çalışılması dünya düzdür demekten öteye gitmemektedir. ISO 27001 bilgi güvenliği standartları kamu kurumları bünyesinde genel kabul görmüş standartları oluşturmaktadır. (ÇEK, E, 2017).

Bilgi güvenliği, bilginin işlenmesi, saklanması, kullanımı, yönetimi ve denetimi ile ilgilidir. BT uyumu ve süreç kontrollerini merkeze almaktadır. Bilgi güvenliğine yönelik riskler, veri güvenliği, erişe bilirliği ve bütünlüğünden taviz verildiği durumlarda ortaya

çıkmaktadır. Etkili güvenlik operasyonları için etkin bir güvenlik mimarisine ihtiyaç duyulmaktadır. Veri gizliliği, kullanılabilirliği ve bütünlüğünün, organizasyon yapısına uygun olması gerekmektedir. Kurumsal güvenlik mimarisi, somut teknik bir araç sağlamasa da gelişmiş tehditler ve saldırılar karşısında iyi bir yol göstericidir. (Ritchot B, 2013)

Kurumsal mimari, tutarlı ilkeler kümesidir. Bilgi güvenliği politikaları çok yönlü bir biçimde ele alınmaktadır. Bilgi güvenliği, dijital ortamda olmayan fiziki verileri de kapsamaktadır. Kurumlar ihtiyaç halinde bilgi güvenliği politikalarında düzenlemeye gidebilir ya da güncelleme yapabilmektedirler. Kurumsal politikalar esnek ve senkronize edilir olmalıdır. Siber güvenlik, sadece uygulamalara yönelik riskleri içermemekte, sosyo-teknik konuları da içermektedir. (Sara Larno, V. S. and a. J. Nurmi (2019).

Güvenlik zafiyetleri; yetersiz şifreleme politikaları, güncel olmayan güvenlik programları, zararlı yazılımlar, bilinçsiz hizmet kullanıcılarının varlığı neticesinde ortaya çıkmaktadır. Güvenlik politikaları, olay yönetimi, iş sürekliliği, güncel sistem yapılanması, kademelendirilmiş güvenlik, kurumsal güvenlik mimarisi yapılanması için operasyonel ve organizasyonel bir boyut kazandırmıştır. (ÇAĞLAR, T. Ö. A, 2020)

6. GÜVENLİK MİMARİSİ HEDEFLERİ

Globalleşen dünyada internetin her alanda yaygın olarak kullanılması risklerin de beraberinde gelmesine neden olmaktadır. İnternetin sunmuş olduğu kolaylıkların arkasındaki tehditlere karşı duyarlı ve uyanık olunması gerekmektedir. Etkin bir güvenlik anlayışı ile standartlar geliştirilmektedir. 2021 yılı içerisinde kamu sektöründe BT' leri yatırımlarına ayrılan bütçe diğer sektörlerden daha fazladır. Farklı zaman dilimlerinde düzenli olarak gerçekleştirilecek güvelik taramaları ile riskler en aza indirilebilmektedir. Entegre güvenlik sistemleri aracılığı ile kurumsal hizmetler kesintiye uğradan hızlı ve güvenli bir biçimde kullanıcıların hizmetine sunulmaktadır. Sürdürülebilir güvenlik politikası çalışmaları, fiziki kültürel çevre, kişisel sanal dünya, kurumsal dijital âlem gerekleri göz önünde bulundurularak oluşturulmaktadır. Siber âlem kişisel ve kurumsal boyutlardan sıyrılarak uluslararası boyutta devletleri bünyesinde barındırmaktadır. İşte bu yüzdendir ki güvenlik, kişisel ve kurumsal olarak ele alınmalı ancak uluslararası çerçevede değerlendirilmelidir. Devletlere ait hassas verilerin koruması için kurumsal güvenlik mimarisi kazanımlarına ihtiyaç duymaktadır. Kurumsal hizmetlerin yürütülmesinde personelin umarsız hareketlerde bulunması güvenlik zafiyetlerine neden olabilmektedir. (Rights, R. F, 2000-2002)

BT ilerlemeleri, devletlerin hizmet portföylerine yönelik avantajlar sağlamaktadır. Dijital hizmetler çeşitlendirerek sunulan hizmet kapasitesi genişletilmektedir. Bütünleşik güvenlik mimarisi çerçeve modelleri aracılığı ile veri güvenliği sağlanarak zamandan, maliyetten ve itibar kayıplarından ödün verilmemektedir. (Digital Economy and Society Index (DESI) 2022)

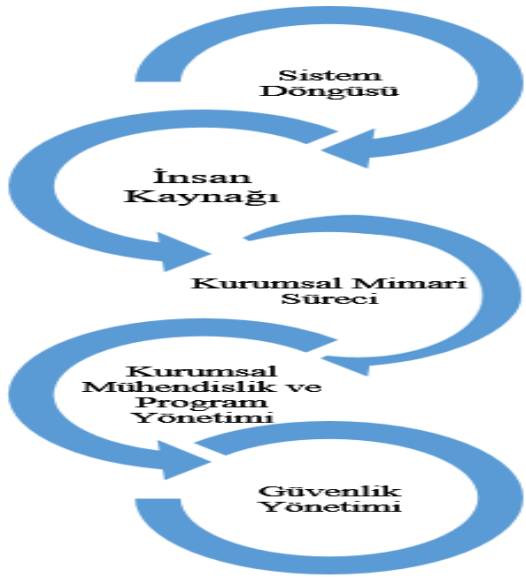
Hayata bakış açımızı bütünüyle değiştiren covid-19 salgını, pek çok alanda olduğu gibi BT'leri yapılanması üzerinde de köklü değişikliklere neden olmuştur. Salgın dönemi içerisinde BT kullanım oranında yaşanan artışla birlikte siber saldırı oranlarında da artış olduğu gözlemlenmiştir. Siber saldırıların önüne geçebilmek adına mevcut güvenlik stratejileri yetersiz kaldığından bütüncül bir kurumsal güvenlik mimarisine ihtiyaç duyulmuştur. Kamusal e devlet hiyerarşisi içerisinde entegre e – hizmetler zamandan ve mekandan bağımsız bir biçimde hareket olanağı sağlamıştır. (Onur Korucu, M.S. LL.M, 2021)

7. DÜNYADA KURUMSAL MİMARİ ÇALIŞMALARI

Siber uzayın genişlemesi ile birlikte kurumsal güvenlik mimarisi devletler için bir ihtiyaç olmaktan çıkarak zorunluluk haline dönüşmüştür. Kurumsal mimari uygulamalarının altyapısı güvenlik mimarisi ile desteklenmektedir. Kurumsal güvenlik hiyerarşisi hesap verebilir, şeffaf ve güvenli ortam basamaklarından oluşmaktadır. Kurumsal mimari, kamusal hizmetlerin sunulması açısından, hedeflerine ulaşabilmek için BT' leri alt yapısından faydalanmaktadır. Evrensel olarak kabul edilen kurumsal güvenlik mimari örneklerinden çalışma kapsamında faydalanılmaya çalışılmıştır. Kurumsal mimari ile farklı bakış açıları ve farklı düzeylerde bağlamsal, kavramsal ve mantıksal soyutlamalar sağlamaktadır.

Güvenlik referans mimari çerçeve seçiminde, ülkelerin gelişmişlik düzeyleri, bilgi toplumuna geçişte hazır oluş seviyeleri, dijital yoğunluk indexleri gibi faktörler göz önünde bulundurulmuştur. Kurumsal mimari, farklı hizmet sektörlerini bütünleştirmede, ortak dil kullanımı ve işbirliğine teşvik etmekte, strateji ve planlama oluşturarak uygulamaları desteklemektedir.

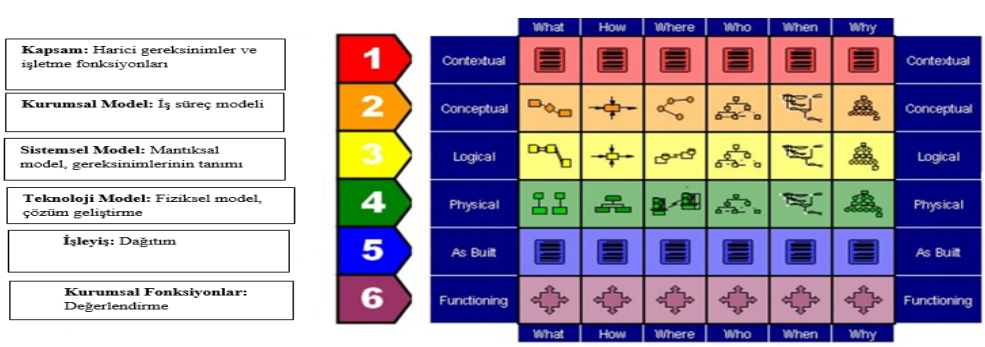
Kurumsal güvenlik mimarisi sürekli güncel tutulması gereken bir yapıya sahiptir. Zachman, DoDAF, TOGAF, SABSA, FEAF, DNDAF, OSI, Gartner vb. çerçeveler, kurumsal güvenlik mimari çalışmalarına örnek olarak gösterilmektedir. Şekil 1' de kurumsal mimari işleyiş yapısına ait döngü gösterilmektedir.



Şekil 1. Kurumsal Mimari Döngüsü (Batdorf, R, 2015)

7.1. ZACHMAN

Zachman, kurumsal mimariyi gruplamak adına ne, nasıl, nerede, kim, ne zaman, neden gibi sorular ile sorular matrisini geliştirmiştir. Basit ve anlaşılır bir yapı oluşturmaya çalışmıştır. Şekil 2' de Zachman kurumsal çerçeve modeline ait kapsam, model, işleyiş ve fonksiyonlar bütüncül bir biçimde verilmeye çalışılmıştır. Zachman çerçevesi ilk kurumsal mimari çalışması olmasından dolay incelemeye esas alınmıştır. Zahman çerçevesi, kurumsal mimari çalışmalarının temelini oluşturması açısından önemli bir yere sahiptir. Değişkenlik gösteren yapıları, bütüncül bir biçimde ele alarak değerlendirmektedir. (BAKANLIĞI, T. C. Ç. V. Ş, 2021).



Şekil 2. Zachman Kurumsal Çerçeve Modeli

7.2. TOGAF

TOGAF, BT leri çerçevesinin, tasarlanıp projeye dönüştürülmesinden, hayata geçirilip yönetilmesine kadar kapsamlı bir yaklaşım biçimini benimsemektedir. TOGAF, süreçler üzerinde etkinlik sağlamaktadır. Stratejik bilgi sistemleri kullanılarak araştırmalar yapılmaktadır. En temel hedefleri iş mimarisi ve boşluk analizleriyle sürdürülebilirliği sağlamaktır. Şekil 3' te TOGAF' ın mimari yapılanmasına ait genel işleyiş yapısı verilmeye çalışılmıştır. TOGAF, günümüz kurumsal mimari örnekleri arasından en çok tercih edilen kurumsal çerçeveyi oluşturmaktadır. BİT' leri ve birimler arası uyum sağlaması açısından önemli bir yere sahiptir. Süreç yönetiminde aktif rol alması, geniş bir kullanım alanına sahip olduğunun göstergesidir. TOGAF dünyada en çok tercih edilen kurumsal mimari örnekleri arasında olmasından çalışmaya esas alınmıştır. TOGAF çerçevesi ADM aracılığı ile süreç, veri entegrasyonu alt yapı ve uygulamalarını ihtiyaçlar doğrultusunda şekillendirmektedir. (Lise Urbaczewski , S. M 2006)

Şekil 3. TOGAF Yapılanması

7.3. SABSA (Sherwood Applied Business Security Architecture)

İş hedeflerini destekleyerek kurumsal güvenliğin sağlanmasında altlık oluşturmaktadır. İş hedefleri doğrultusunda risklerin analizleri yapmaktadır. Güvenliğe yönelik ihtiyaçlar doğrultusunda politikalar geliştirilmeye çalışılmaktadır. Risk değerlendirmeleri kurumsal mimarinin güvenlik gereksinimleri hizmet ve uygulama yönüne göre belirlenmektedir. (Madsen, T, 2022)

Güvenlik Hizmet Yönetimi Mimarisi (SABSA MODELİ)

- Bağlamsal güvenlik mimarisi
- Kavramsal güvenlik mimarisi
- Mantıksal güvenlik mimarisi
- Fiziksel güvenlik mimarisi
- Bütünleşik güvenlik mimarisi

7.4. AUSDAF

Avustralya hükümeti bireyden topluma her kesimi kapsamayan genel bir, güvenli oluşum platformu, oluşturma çalışmaları yürütmektedir. Bilgi güvenliği konusunda halkı bilinçlendirmek adına bir kılavuz hazırlamışlardır. Duyarlı ve bilinçli bir toplum yaratılmaya çalışılmaktadır. Güvenliğe yönelik hizmet anlayışı içerisinde standartlar geliştirilmektedir. Güvenlik tehditleri ve unsurları resmi web siteleri aracılığıyla duyurular kısmında herkese ilan edilmektedir. Dış saldırılara karşı, yazlım ve donanım altyapısı güvenliğinin güncel ve aktif tutulması gerekliliğine vurgu yapmaktadır. Kritik öneme sahip veriler gruplandırılmaktadır. (https://www.cyber.gov.au/acsc/view-all-content/ism)

	Ulusal Bilgi Güvenliği Standartları ve Stratejileri	Kurumsal Risk Yönetimi Analizleri	Kurumsal bilgi güvenliği platformu	Ulusal Bilgi güvenliği kılavuzu	Risk yönetiminde sistem geri bildirimi sağlama	Kimlik doğrulama ve yetkilendirme
AVUSTRALYA	X	X	X	X	X	X
ESTONYA	X	X	X		X	X
HİNDİSTAN	X	X	X		X	X
KOLOMBİYA	X	X	X	X	X	X
HOLLANDA	X	X	X		X	X

Tablo.1. Ülkeler Güvenlik Mimari karşılaştırması

7.4 -7.8 arasında, 2018-2020 Birleşmiş Milletler, ülkelerin E devlet gelişmişlik indeksi raporuna göre; E devlet gelişmişlik endeksi çok yüksek olan ülkelere Danimarka, Estonya ve Avustralya vb. örnek olarak verilebilmektedir. Aynı raporda yer alan, Hindistan ve Kolombiya' da yüksek e- gelişmişlik endeksine sahip ülkeler arasındadır. Çalışmaya yol göstermesi açısından e devlet gelişmişlik indeksi yüksek olan ülkelerden faydalanılmıştır. (Zhenmin, L, 2020)

6.5. ESTONYA

Estonya dijital dönüşüme hızlı bir biçimde adapte olmuştur. Bünyesinde sunmuş olduğu e- hizmetler aracılığı ile de bu değişimi gözler önüne sermiştir. E –hizmet uygulamaları dijital kimlikler vasıtası ile sürdürülmektedir. Hizmet bütünlüğü içerisinde kullanıma sunulan uygulamalar aşamalı bir güvenlik temeline dayandırılmıştır. Veri bütünlüğü sağlanmaya çalışılır iken veri tekrarlarının da önüne geçilmektedir. Kişisel veriler devlet eli ile temel hak ve hürriyetler kapsamında değerlendirilmektedir. Kişisel

dijital kimliklerin ardından, e imzanın da kullanıma sunulmasıyla dijital veriler de kimlik kazanmış oldu. Estonya hükümeti güvenlik söz konusu olduğunda kesin çizgiler üzerinde hareket etmektedir. Uygulamalar ihtiyaçlar ölçüsünde yenilenmektedir. Uygulamaların işlevsel ve kullanılabilir olması da son derece önem arz etmektedir. E devlet uygulamaları, güvenliği esas almaktadır. Kurumlar e- devlet uygulamaları aracılığı ile sistem üzerinden veri güncellemesi yaparak vatandaşlara en iyi hizmeti sunmaktadırlar. (Vassil, K, 2015).

7.6. HİNDİSTAN

Hindistan, web ve mobil uygulamalar aracılığı ile e-hizmetlerini vatandaşlarına ilan etmekte ve hayata geçirmektedir. Merkeziyetçi bir yapı içerisinde benzer uygulamaların tekrarını ortadan kaldırmaktadır. Merkeziyetçi yapının altındaki denetim mekanizması ile referans mimari kontrol altında tutulmaktadır. Ülke kurumsal mimari duruşunu gerçekleştirmek adına bir takım standartlar ve ilkeler benimsemiştir. Hizmetler kurumsal bir ara yüz ile vatandaş odaklı olarak güvenlik ve gizliliğin esas alındığı bir çerçevede sunulmaktadır. Sürdürülebilir kalkınma hedefleri öncelik sırasına göre ele alınmaktadır. Uygulamalarla ortak bir alt yapı içerisinde birlikte çalışabilirlik hedeflenmektedir. (Sachdeva, S, 2019)

7.7. KOLOMBİYA

Kolombiya hükümeti geliştirmiş olduğu standart ve politikalar aracılığı ile kurumsal bir olgunluk modeli oluşturmuştur. Oluşturulan model aracılığı ile en yüksek faydaya ulaşma arzusu dile getirilmiştir. Bilgi güvenliği standart ve politikaları, birlikte çalışabilirlik, şeffaflık, hesap verebilirlik, gizlilik, bütünlük ve erişilebilirlik göz önünde bulundurularak oluşturulmuştur. Avustralya, Singapur ve İngiltere kurumsal mimarilerinden etkilenilerek Kolombiya kurumsal mimarisi oluşturulmuştur. BT' leri yatırımlarına yönelik etkin bir maliyet sistemi oluşturulmaya çalışılmaktadır. Kişisel ve kurumsal verilere ait güvenliği ön planda tutmaktadırlar. Dijital devlet politikası gereği mimari çerçeve BT' leri yönetim modeli ile doğrudan etkileşim içerisindedir. ("Arquitectura Gubernamental de Australia - AGA." from).

7.8. HOLLANDA

ISO 207001 standartları doğrultusunda bilgi güvenliği politikaları uygulanılmaya çalışılmaktadır. Dijitalleşmenin sağlamış olduğu uygulama avantajları, e devlet yapısı ile bir bütünlük kazanmıştır. Güvenlik tek aşamalı olarak ele alınmamaktadırlar. Hizmet bütünlüğü açısında, her aşamada temel güvenlik tedbirleri uygulanmaya çalışılmaktadır. AB Birlikte Çalışabilirlik Referans Mimarisine ters düşmeyecek şekilde çerçeve mimari oluşturulmaya çalışılmıştır. Bu yapılanma ile bütünleşik bir hizmet anlayışı ortaya çıkmıştır. TOGAF kurumsal mimarisinden esinlenilmiştir. Sosyal ve toplumsal değerler, en etkin güvenlik kültürünün oluşturmada önemli bir rol oynamaktadır. ("The Dutch Governmental Reference Architecture". from).

	Zachman	TOGAF	SABSA	Avustralya	Estonya	Hindistan Indea	Kolombiya	Hollanda (NORA)
İş Katmanı		X	X	X	X	X	X	X
Entegrasyon Katmanı	X	X	X	X	X	X	X	X
Veri Katmanı	X	X	X	X	X	X	X	X
Altyapı cihaz Katmanı	X	X	X	X	X	X	X	X
Uygulama Katmanı	X	X	X	X	X	X	X	X
Güvenlik Katmanı	X	X		X	X	X	X	X
Ağ İletişimi				X	X		X	X
Standartlar				X	X	X	X	X

Tablo.2. Güvenlik Mimarileri Karşılaştırması

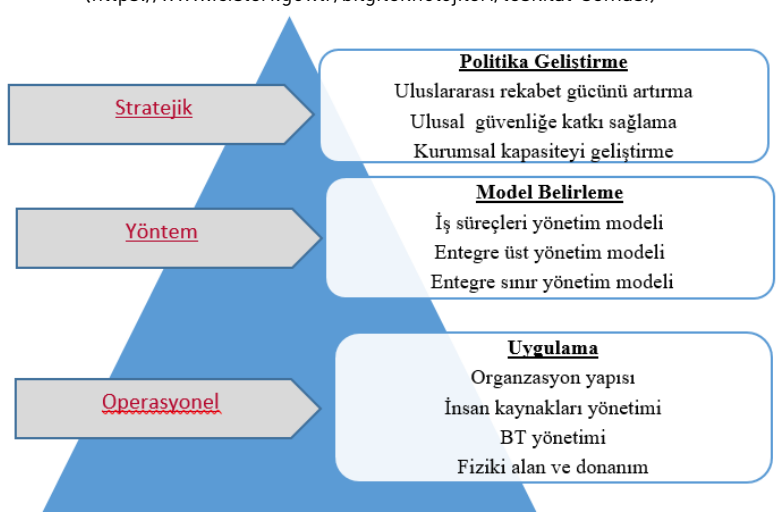
Ülkelerin, kurumsal mimari çerçevelerini katmanlı yapılar, standartlar ve ağ iletişim yapılarıyla destekledikleri görülmektedir.

8. DÜNYA ODAĞINDA TÜRKİYE İNCELEMESİ

Ülkemizde bilgi güvenliğine yönelik çalışmalar; SOME, BGYS, KamuNET, KVKK, CB-DDO, UAB vb. kurumlar aracılığı ile yürütülmektedir. Kurumsal mimari genel yapısı, stratejik hedefleri ve kurumsal kazanımları ile birlikte ele alınmaktadır. Şekil 4' ten de anlaşılacağı üzere bütün katmanlarda güvenlik ele alınmıştır. Şekil 5' te İçişleri Bakanlığı' nın, bilgi teknolojileri güvenliğine yönelik yapılanması gözler önüne serilmiştir.

Şekil 4. İçişleri Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü Teşkilat Yapısı

(https://www.icisleri.gov.tr/bilgiteknolojileri/teskilat-semasi)



Şekil 5. Ticaret Bakanlığı Kurumsal Mimari Emsal Model (ŞEN F, 2018)

9. SONUÇ

Dijital hizmet odaklı dönüşümler, kullanıcılara sanal dünyanın kapılarını aralamıştır. Kamu kurum ve kuruluşları arşivlerindeki kurumsal ve kişisel veriler, bilişim sistemleri aracılığı ile üzerinde titizlikle çalışılarak korunmaktadır. Bilgi güvenliği açısından riskler ortadan kaldırılamıyor ise zararları en aza indirilmeye çalışılmalıdır. Kurumsal mimari çalışmaları ile iş sürekliliği sağlanmaktadır. Kurumsal referans güvenlik mimarisi yaklaşımları ile güvenlik bütün boyutları ile ele alınmaktadır. Yetişmiş insan gücü eksikliği, ar-ge faaliyetleri için yeterli bütçe ayrılmaması, yasal çerçevenin tam anlamıyla oturtulmaması, denetimlerin zamanında gerçekleştirilmemesi, teknik altyapının gereksinimler ölçüsünde yenilenmemesi, kişisel bilgi güvenliğinin sağlanmasında umarsız davranılması, düzenli aralıklar ile güvenlik farkındalığı eğitimlerinin gerçekleştirilmemesi vb. durumlardan dolayı güvenliğin sağlanmasında aksaklıklar yaşanmaktadır. Bilgi toplumu temel felsefesi içerisinde şeffaflık, hesap verebilirlik, sürdürülebilirlik ve erişilebilirlik önemli bir etki alanına sahiptir. Kurumsal güvenlik mimarisi kurumsal hiyerarşi içerisinde etkinlik, verimlilik ve bütünlük sağlamaktadır. Kurumsal referans güvenlik mimarisi iş, veri, uygulama ve altyapı mimarileri çerçeve bakış açıları doğrultusunda hareket edebilmektedir. Güvenlik mimarisi, temel güvenlik bakış açısıyla da bütüncül bir biçimde ele alınabilmektedir. Ülkemizde de bilgi ve bilişim teknolojileri güvenliğine yönelik kurumsal yönden çalışmalar yürütülmektedir. Ülkelerin gelişmişlik düzeyleri mimari model seçiminde etkili olabilmektedir. Benzer güvenlik fonksiyonları ilişkilendirilerek farklı açılardan avantajlar sunabilmektedir.

Araştırmaya konu olan kurumsal güvenlik mimarisi kurumsal hizmet bütünlüğü çerçevesinde veri güvenliğine yönelik olarak sürekli güncel ve geliştirilebilir olmalıdır. Salgın süresince kamu kurumları, vatandaşlara dijital teknolojiler aracılığı ile daha hızlı bir biçimde ulaşmaya çalışmıştır.

Çalışmanın amacı kapsamında, dünyadaki kurumsal mimari örnekleri incelenmiş ve gelişmiş ülkelerde dijitalleşmenin bir sonucu olarak kamu kurumlarının kapsamlı ve bütüncül bir milli kurumsal güvenlik mimarisine ihtiyaç duydukları sonucuna ulaşılmıştır. Vatandaş odaklı sunulan dijital hizmetlerde amaçları, hedefler ve sürdürebilirlik ilkeler olgunlaştırmaktadır. Kurumsal mimari çalışmaları yürütülür iken ülkelerin politik, kültürel ve sosyal faktörlerinin göz önünde bulundurulması gerekmektedir. Avustralya kurumsal mimarisinde olduğu gibi milli ve kurumsal bilgi güvenliği kılavuzu oluşturarak riskler konusunda kullanıcılar bilinçlendirilebilmelidir. Benzer riskler açısında ortak bir akıllı cihaz uygulaması platformu oluşturularak hizmet etkileşim kalitesi artırılabilmektedir.

Estonya, güvenliği bütün katmanlarında ele alarak üst düzey koruma sağlamaya çalışmıştır. Güvenlik mimarisi çalışmalarında kompleks yönetim anlayışıyla sorunları basitleştirmektedir. Güvenlik ve dijital dönüşüme duyarlı bir kurumsal mimari ile

kurumsal e-hizmetler şeffaf olarak daha geniş kitlelerin kullanımına sunulmaktadır.

Hindistan, kurumsal güvenliği merkez alan çerçeve yaklaşımlar aracılığıyla sürdürülebilir dijital hizmetleri denetlenebilmektedir. Merkeziyetçi bir yapıya sahiptir.

Hollanda, referans mimari modeller taksonomileri, güvenlik mimarilerine yönelik ortak çıkarımlar sunmaktadır. Çekirdek güvenlik mimarisi aracılığı ile veri güvenliğinde denetimli erişim sağlamaya çalışılmaktadır.

Kolombiya, kurumsal güvenlik mimarisinin temel amacı, kamusal hizmetler aracılığı ile mevcut teknolojiden en iyi şekilde faydalanmak ve bilgi güvenliği hedeflerine ulaşmayı kolaylaştırmaktır. Hollanda ve Kolombiya örneklerinde olduğu gibi farklı çerçevelerin bakış açılarından faydalanılması gerekmektedir. Çerçeve mimari oluşturulur iken bütüncül, sürdürülebilir ve çözüm odaklı ilkeler özelinde eksiklikler gözetilerek çerçeve mimari oluşturulmalıdır.

Ülkemizde kurumsal hizmet anlayışı içerisinde kurumsal mimari yapılanması istenilen noktada değildir. Dijital bir platform oluşturularak riskler konusunda vatandaşlar bilinçlendirilebilir. Kurumsal hizmetlerin bütünüyle e devlet entegrasyonu ile bütünleştirilerek, kurumsal güvenlik ve şeffaflık sağlanmalıdır. Güvenlik her aşamada sağlanmalıdır. Entegre e devlet uygulamalarının ihtiyaçlar ölçüsünde geliştirilmesi ve kişisel ve kurumsal veri güvenliğine gerekli özenin gösterilmesi gerekmektedir. Kamu yönetimi perspektifinde kurumsal ve güvenlik mimarisine yönelik yeterli çalışmanın bulunmamasından dolayı, bu çalışma literatür için iyi bir örnek teşkil edebilmektedir.

Etik Beyanı: Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazarlar beyan eder. Aksi bir durumun tespiti halinde Kamu Yönetimi ve Teknoloji Dergisi'nin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarlarına aittir.

Yazar Katkıları: Sibel KARAKUŞ ÖZTÜRK, İhsan Tolga MEDENİ, Tunç Durmuş MEDENİ ve Mehmet Serdar GÜZEL çalışmanın tüm bölümlerinde ve aşamalarında katkı sağlamışlardır. Yazarlar esere eşit oranda katkı sunmuştur.

Çıkar Beyanı: Yazarlar ya da herhangi bir kurum/ kuruluş arasında çıkar çatışması yoktur.

Teşekkür: Yayın sürecinde katkısı olan hakemlere teşekkür ederiz.

Ethics Statement: The authors declare that the ethical rules are followed in all preparation processes of thisstudy. In the event of a contrary situation, the Journal of Public Administration and Technology has noresponsibility and all responsibility belongs to the author of the study.

Author Contributions: Sibel KARAKUŞ ÖZTÜRK, İhsan Tolga MEDENİ, Tunç Durmuş MEDENİ ve Mehmet Serdar GÜZEL have contributed to all parts and stages of the study. The authors contributed equally to the study.

Conflict of Interest: There is no conflict of interest among the authors and/or any institution.

Acknowledgement: We would like to thank the referees who contributed to the publication process.

KAYNAKÇA

(BAKANLIĞI , BAŞARANOĞLU 11/05/2020, Rights 2000-2002, Lise Urbaczewski 2006, WIKIPEDIA 2006, Ritchot 2013, Çözümleri 2015, Vassil 2015, İnce 2016, 2017, Ayşe MENTEŞE 2017, ÇEK 2017, Jeganathan 2017, KAYA 2017, Rahman 2017, Wahe 2017, GÜMÜŞ 2018, Nather 2018, ŞEN 2018, Sachdeva 2019, Sara Larno and Nurmi 2019, ÇAĞLAR 2020, Zhenmin 2020, Çiftçi 2021, İLHAN and YELKENCİ 2021, Onur Korucu 2021, 2022, BÜLBÜL 2022, Madsen 2022)

"Arquitectura Gubernamental de Australia - AGA." from (https://www.mintic.gov.co/gestion-ti/Arquitectura-TI/Experiencia-Internacional/6059:Arquitectura-Gubernamental-de-Australia-AGA

(2017). "The Dutch Governmental Reference Architecture from https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/solution/eif-toolbox/dutch-governmental-reference-architecture-nora.

(2022). "The Digital Economy and Society Index (DESI)." from https://digital-strategy.ec.europa.eu/en/policies/desi.

Ayşe MENTEŞE , İ. G. Ö., Yenal ARSLAN (2017). A MODEL PROPOSAL FOR ENTERPRISE ARCHITECTURE FRAMEWORK IN SOCIAL SECURITY INSTITUTION Dergipark. TURKEY. **3:** 14.

BAKANLIĞI, T. C. İ. "TEŞKİLAT ŞEMASI." from https://www.icisleri.gov.tr/bilgiteknolojileri/teskilat-semasi.

BAŞARANOĞLU, E. (11/05/2020). "Erişim Kontrolleri Bakışı İle Güvenlik Modelleri" https://www.siberportal.org/white-team/securing-information/erisim-kontrolleri-bakisi-ile-guvenlik-modelleri/.

BÜLBÜL, S. M. H. İ. (2022). "Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Etkinliğinin Analiz Edilmesi." Dergipark: 329.

ÇAĞLAR, T. Ö. A. (2020). «TÜRK KAMU SEKTÖRÜNDE BİLGİ VE BİLİŞİM GÜVENLİĞİ.» Dergipark 22.

ÇEK, E. (2017). KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİŞİMİ VE BİLGİ GÜVENLİĞİ İÇİN İNSAN FAKTÖRÜNÜN ÖNEMİ. BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI. İSTANBUL, İSTANBUL BİLGİ ÜNİVERSİTESİ.

ÇEK, E. (2017). KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİŞİMİ VE BİLGİ GÜVENLİĞİ İÇİN İNSAN FAKTÖRÜNÜN ÖNEMİ

BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

İSTANBUL, İSTANBUL BİLGİ ÜNİVERSİTESİ.

Çiftçi, E. (2021). DEĞİŞEN, DİJİTALLEŞEN VE KÜRESELLEŞEN DÜNYADA GÜVENLİK KAVRAMI 22.

Çözümleri, H. B. (2015). Kurumsal Bilgi Sistemleri Mimarisi Yol Haritası

Harezmi Bilişim Çözümleri

ANKARA, ANKARA**:** 32.

GÜMÜŞ, C. (2018). KURUMSAL MİMARİ ÇERÇEVE YÖNETİMİ'NİN VERİMLİLİĞE ETKİSİ: BANKACILIK SEKTÖRÜNDE UYGULAMALI BİR ARAŞTIRMA İŞLETME ANABİLİM DALI

İSTANBUL, HALİÇ ÜNİVERSİTESİ.

İLHAN, E. and Ö. F. YELKENCİ (2021). YÜKSEKÖĞRETİMDE YENİ MODEL ARAYIŞINDA BÜTÜNLEŞİK BİR TASARIM ÖNERİSİ: DİSİPLİNLERARASI DİJİTAL MODEL**:** 1-22.

İLHAN, E. and Ö. F. YELKENCİ (2021). YÜKSEKÖĞRETİMDE YENİ MODEL ARAYIŞINDA BÜTÜNLEŞİK BİR TASARIM ÖNERİSİ: DİSİPLİNLERARASI DİJİTAL MODEL 1-22.

İnce, A. B. (2016). KURUMSAL GÜVENLİK İNCELEMESİ VE BİR ÇÖZÜM ÖNERİSİ Bilgisayar Mühendisliği Programı İSTANBUL, İSTANBUL TEKNİK ÜNİVERSİTESİ.

Jeganathan, S. (2017). "Enterprise Security Architecture: Key for Aligning Security Goals with Business Goals." ISSA.

KAYA, Ö. F. (2017). KURUMSAL İŞLETMELERDE BİLGİ VE VERİ GÜVENLİĞİ. FEN BİLİMLERİ ENSTİTÜSÜ İSTANBUL, İSTANBUL TİCARET ÜNİVERSİTESİ 14-57.

Lise Urbaczewski , S. M. (2006). "A COMPARISON OF ENTERPRISE ARCHITECTURE FRAMEWORKS ": 23.

Madsen, T. (2022). "3 Security Architecture Model." 30.

Nather, S. (2018). Improving Information Security Through Risk Management and Enterprise Architecture Integration.

Onur Korucu, M. S., LL.M (2021). "YENİ NORMAL DÜNYA DÜZENİNİN SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİNE ETKİLERİ." Dergipark: 46.

Rahman, M. T. U. A. N. I. B. M. M. (2017). "A secure enterprise architecture focused on security and technology-transformation (SEAST)." IEEE.

Rights, R. F. (2000-2002). "GIAC CERTIFICATIONS." 12.

Rights, R. F. (2000-2002). "Global Information Assurance Certification Paper." GIAC CERTIFICATIONS: 12.

Ritchot, B. (2013). "An Enterprise Security Program and Architecture to Support Business Drivers." TIM Review: 33.

Sachdeva, S. (2019). "India Enterprise Architecture: What is it and should it be made mandatory for all e-governance projects?".

Sara Larno, V. S. and a. J. Nurmi (2019). "Method Framework for Developing Enterprise Architecture Security Principles." Complex Systems Informatics and Modeling Quarterly (CSIMQ)(20): 71.

ŞEN, F. (2018). «Kurumsal Mimari ve Stratejik Konumlandırma: Gümrük ve Ticaret Bakanlığı Örneği.» Dergipark: 12.

Vassil, K. (2015). Estonian e-Government Ecosystem**:** 1-30.

Wahe, I. U. M. A. S. A. W. A. (2017). "Protection of enterprise resources: A novel security framework." IEEE.

Zhenmin, L. (2020). E-Government Survey 2020**:** 1-323.