İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 21(42), Güz 2022, 353-382.

İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Araştırma Makalesi / Research Article

ULUSAL BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ: IoT GÜVENLİĞİ İÇİN BİR UYGULAMA ÖRNEĞİ*

NATIONAL INFORMATION AND COMMUNICATION SECURITY GUIDE: AN APPLICATION EXAMPLE FOR IoT SECURITY

Muttalip TULGAR[1] **Abdül Halim ZAİM[2]** **Muhammed Ali AYDIN[3]**

https://doi.org/10.55071/ticaretfbd.1141795

Sorumlu Yazar / Corresponding Author
muttalip.tulgar@istanbulticaret.edu.tr

Geliş Tarihi / Received
07.07.2022

Kabul Tarihi / Accepted
12.08.2022

Öz

Kamu kurumları ve kritik altyapı hizmeti veren işletmelerce uyulması gereken bilgi güvenliği tedbirlerini içeren Ulusal Bilgi ve İletişim Güvenliği Rehberi, ülkemize özgü ilk referans doküman olma niteliği taşımaktadır. Rehber, bilgi ve iletişim güvenliği alanındaki büyük bir boşluğu doldurmakla birlikte, kurumların siber saldırılara karşı dayanıklılığını artırmada da önemli bir özelliğe sahiptir. Bu çalışmada, Rehber'in genel yapısı incelenerek rehber uygulama süreçleri hakkında bilgi verilmektedir. Ayrıca Rehber kapsamında ele alınan ve ana başlıklardan biri olan Nesnelerin İnterneti (IoT) güvenliğine yönelik siber güvenlik saldırıları ve zafiyetlerine değinilmiştir. Bu çalışmada simülasyon ortamında temsili bir kurumsal yapının ağ topolojisi oluşturularak rehberdeki IoT güvenliği denetimlerinin nasıl yapılacağı gösterilmektedir. Güvenlik denetimleri ile temsili kurumun rehberde yer alan IoT güvenliğine yönelik tedbirlere uyumunun sağlanması amaçlanmaktadır.

Anahtar Kelimeler: Bilgi güvenliği, bilgi ve iletişim güvenliği rehberi, güvenlik denetimi, IoT, nesnelerin interneti, siber güvenlik.

Abstract

In this study, a questionnaire study conducted to organizations that The National Information and Communication Security Guide, which includes information security measures to be followed by the public institutions and the operators providing critical infrastructure services, is the first reference document specific to our country. Along with filling a big gap in the field of information and communication security, the guide also has an important feature in increasing the resilience of institutions against cyber attacks. In this study, the general structure of the guide is examined and information about the guideline implementation processes is given. In addition, cyber security attacks and vulnerabilities for Internet of Things (IoT) security, which is one of the main topics covered in the guide, are mentioned. In this study, it is shown how to perform the IoT security audits in the guide by creating the network topology of a representative corporate structure in the simulation environment. With security audits, it is aimed to ensure the compliance of the representative institution with the measures for IoT security in the guide.

Keywords: Cyber security, information security, information and communication security guide, internet of things, IoT, security audit.

**Bu yayın Muttalip TULGAR isimli öğrencinin İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Programındaki Lisansüstü tezinden üretilmiştir.*

[1]İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul, Türkiye.
muttalip.tulgar@tubitak.gov.tr, Orcid.org/0000-0001-9151-474.

[2]İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye.
azaim@ticaret.edu.tr, Orcid.org/0000-0002-0233-064X.

[3]İstanbul Üniversitesi- Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye
aydinali@istanbul.edu.tr, Orcid.org/0000-0002-1846-6090.

1.GİRİŞ

Bu çalışmada, ülkemize özgü olarak hazırlanmış ve bilgi güvenliği tedbirleri konusunda referans teşkil edebilecek ilk doküman olma özelliği taşıyan Bilgi ve İletişim Güvenliği Rehberi'nin genel yapısı ve içeriği hakkında bilgi verilerek Rehber uygulama süreçlerinin her bir adımına dair açıklamalarda bulunulmuştur. Rehber'de birçok ana başlık ve çok fazla güvenlik tedbiri olduğu için çalışma kapsamında daraltmaya gidilmiş sadece Rehber'deki ana başlıklardan biri olan Nesnelerin İnterneti (IoT) güvenliğine yönelik siber güvenlik tedbirleri ele alınmıştır. Bu çalışmanın diğer bir amacı da IoT ortamlarının güvenliğinin nasıl sağlanabileceğine dair bir uygulama platformu oluşturmaktır. Özellikle IoT sistemleri için test ortamı oluşturmanın zorluğu ve herhangi bir kurumun aktif çalışan IoT ortamında güvenlik denetimi yapmasının yüksek risk barındırması nedeniyle simülasyon ortamına ihtiyaç bulunmaktadır. Bu çalışmada da Cisco Packet Tracer yazılımı kullanılarak simülasyon ortamı oluşturulmuş ve temsili bir kurumsal yapının Rehber ile uyumlu olup olmadığı IoT güvenliği özelinde gösterilmiştir.

2. LİTERATÜR ARAŞTIRMASI

Literatür taramalarında, Ulusal Bilgi ve İletişim Güvenliği Rehberi'ne yönelik herhangi bir çalışmaya rastlanmamıştır. Rehber'e yönelik tek atıf, Ağdeniz (2021) tarafından yapılmış olup yazar çalışmasında kamu iç denetçilerinin yılda en az bir kez Bilgi ve İletişim Güvenliği Rehberi kapsamında denetim yapma zorunluluğundan bahsetmiştir.

Zeybek & Yılmaz (2019) yaptıkları çalışmada, iç denetçilerin IoT cihazlarının çeşitliliği ve yapısal zorlukları nedeniyle doğru güvenlik yaklaşımları, risk yönetimi ve genel bir denetim metodolojisi belirleyerek kurum güvenlik kültürüne değer katabileceklerini vurgulamışlardır.

Kaymas (2020), Türkiye'de nesnelerin interneti ekosisteminin gelişmesi için kamusal politikaların yeniden gözden geçirilmesini ve başta üniversite ve araştırma merkezleri olmak üzere ulusal inovasyon ağının kurulması gerektiğini önermiştir.

Ülker ve ark. (2017), IoT sistemlerinin birçok kamu kurumunda kullanıldığını, bu sistemlerin de diğer bilişim teknolojilerinde kullanılan bileşenler gibi siber saldırılara maruz kalarak ulusal bilgi güvenliğini tehdit ettiğini, bu nedenle IoT güvenliğine özgü güvenlik politikalarının uygulanması gerektiğini vurgulamıştır.

Avcı (2022), çalışmasında akıllı evlerde kullanılan IoT teknolojileri ve IoT güvenlik katmanlarını incelemiş, IoT sistemlerinde en çok yaşanan 10 güvenlik sorununa değinmiştir. Yazar, IoT güvenliğinin sağlanabilmesinin ancak bütüncül bir güvenlik anlayışı ile mümkün olabileceğine bu nedenle sistemin tüm bileşenlerinin güvenlik risklerinin iyi analiz edilmesinin önemine değinmiştir.

Thera (2020) tez çalışmasında öğrencilerin IoT ağlarını daha iyi anlaması ve rahatlıkla bir IoT ortamı oluşturabilmesi için akıllı ev ortamını Cisco Packet Tracer ile oluşturmuştur.

Özdoğan & Daş (2021), Cisco Packet Tracer simülasyon ortamında akıllı ev otomasyon sistem tasarımı için 3 farklı senaryo geliştirmiş ve farklı senaryolara göre araçların kullanımını örneklerle göstermişlerdir.

3. ULUSAL BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ

Bilgi ve İletişim Güvenliği Rehberi'nin adı, ilk kez 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 2019/12 sayılı Cumhurbaşkanlığı Genelgesi'nde yer almıştır. T.C. Dijital Dönüşüm Ofisi Başkanlığı tarafından Temmuz 2020 yılında yayımlanan Rehber, bilgi işlem birimi bulunan veya bilgi işlem hizmetlerini üçüncü taraflardan alan kamu kurumları ile kritik altyapı niteliğinde faaliyet gösteren işletmelerin uyması gereken güvenlik tedbirlerinden bahsetmektedir (DDO, 2020).

3.1. Rehber İçeriği

Rehber; 229 sayfa, 661 güvenlik tedbiri ve 4 temel bölümden oluşmaktadır:

- Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci: Bilgi güvenliği yönetim süreçlerinin Rehber özelinde uygulandığı ve güvenlik tedbirlerinin yerine getirilmesinde uygulanacak yöntemlerin bahsedildiği bölümdür.

- Varlık Gruplarına Yönelik Güvenlik Tedbirleri: Rehber'de tanımlanan varlık grubu ana başlıklarına yönelik güvenlik tedbirlerinin yer aldığı bölümdür. Tablo 1.'de varlık gruplarına yönelik güvenlik tedbirleri alt başlıkları görülmektedir. Bu alt başlıklara yönelik toplam 416 güvenlik tedbiri bulunmaktadır.

Tablo 1. Varlık gruplarına yönelik güvenlik tedbirleri alt başlıkları

Ağ ve Sistem Güvenliği
Donanım Varlıklarının Envanter Yönetimi
Yazılım Varlıklarının Envanter Yönetimi
Tehdit ve Zafiyet Yönetimi
E-Posta Sunucusu ve İstemcisi Güvenliği
Zararlı Yazılımlardan Korunma
Ağ Güvenliği
Veri Sızıntısı Önleme
İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi
Sanallaştırma Güvenliği
Siber Güvenlik Olay Yönetimi
Sızma Testleri ve Güvenlik Denetimleri
Kimlik Doğrulama ve Erişim Yönetimi
Felaket Kurtarma ve İş Sürekliliği Yönetimi
Uzaktan Çalışma
Uygulama ve Veri Güvenliği
Kimlik Doğrulama
Oturum Yönetimi
Yetkilendirme
Dosyaların ve Kaynakların Güvenliği
Güvenli Kurulum ve Yapılandırma
Güvenli Yazılım Geliştirme
Veri Tabanı ve Kayıt Yönetimi
Hata Ele Alma ve Kayıt Yönetimi
İletişim Güvenliği
Kötücül İşlemleri Engelleme
Dış Sistem Entegrasyonlarının Güvenliği

Taşınabilir Cihaz ve Ortam Güvenliği
Akıllı Telefon ve Tablet Güvenliği
Taşınabilir Bilgisayar Güvenliği
Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
Ağ Servisleri ve İletişimi
Dâhili Veri Depolama
Kimlik Doğrulama ve Yetkilendirme
API ve Bağlantı Güvenliği
Diğer Güvenlik Tedbirler
Personel Güvenliği
Genel Güvenlik Tedbirleri
Eğitim ve Farkındalık Faaliyetleri
Tedarikçi İlişkileri Güvenliği
Fiziksel Mekânların Güvenliği
Genel Güvenlik Tedbirleri
Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri
Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)

- Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri: Bu bölümde Tablo 2.'de gösterilen varlık gruplarındaki ana başlıklar için uygulanması düşünülen, uygulama ve teknoloji alanlarına yönelik 146 tedbir maddesi bulunmaktadır.

Tablo 2. Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri alt başlıkları

Kişisel Verilerin Güvenliği
Kayıt Yönetimi
Erişim Kayıtları Yönetimi
Yetkilendirme
Şifreleme
Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme
Aydınlatma Yönetimi
Açık Rıza Yönetimi
Kişisel Veri Yönetim Sürecinin İşletilmesi
Anlık Mesajlaşma Güvenliği
Genel Güvenlik Tedbirleri
Bulut Bilişim Güvenliği
Genel Güvenlik Tedbirleri
Kripto Uygulamaları Güvenliği
Kriptografik Algoritmalar ve Kullanımı
Şifreleme ve Anahtar Yönetimi
Kriptografik Uygulamalar
Kritik Altyapılar Güvenliği
Genel Güvenlik Tedbirleri
Enerji Sektörü Özelinde Güvenlik Tedbirleri
Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri
Yeni Geliştirmeler ve Tedarik Genel Güvenlik Tedbirleri
Genel Güvenlik Tedbirler

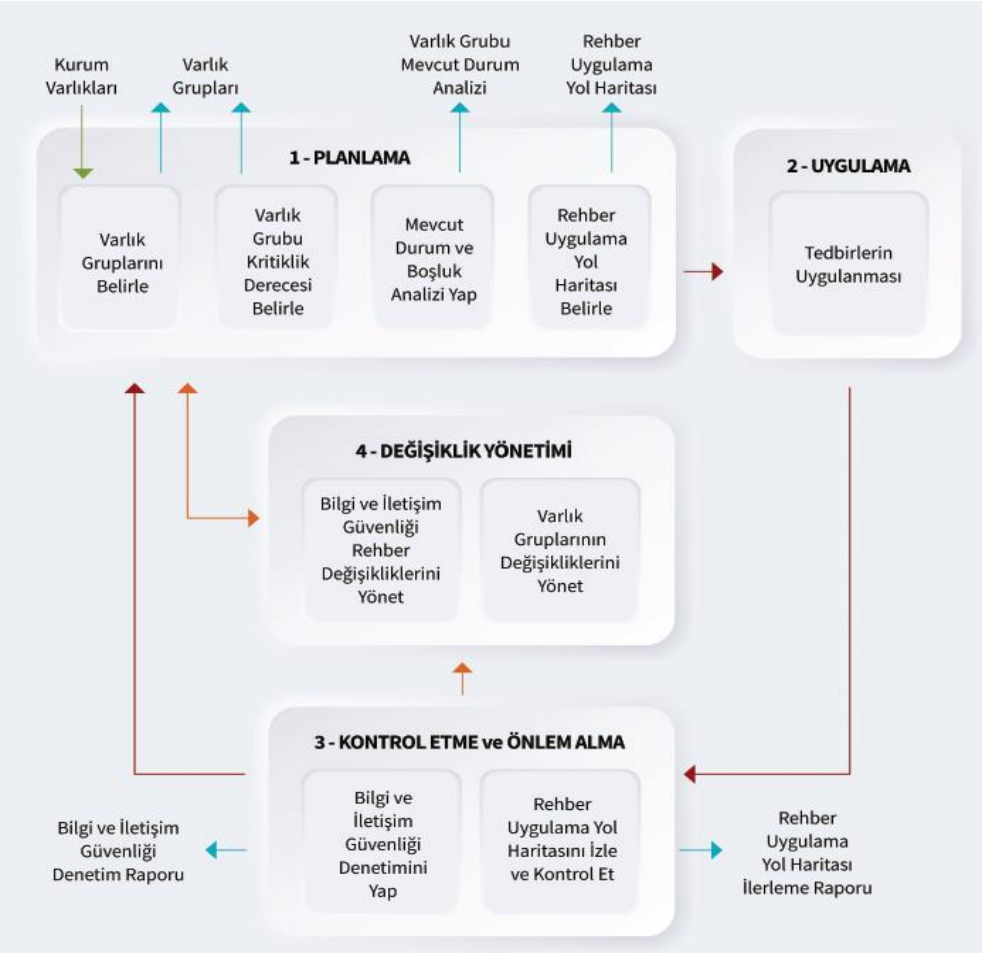
- Sıkılaştırma Tedbirleri: Bu bölümde işletim sistemleri, veri tabanı ve sunucu sıkılaştırmalarının bulunduğu 99 adet güvenlik tedbiri yer almaktadır. Tablo 3.'de sıkılaştırma tedbirlerine yönelik alt başlıklar görülmektedir.

Tablo 3. Sıkılaştırma tedbirlerine yönelik alt başlıklar

İşletim Sistemi Sıkılaştırma Tedbirleri
Genel Sıkılaştırma Tedbirleri
Linux İşletim Sistemi Sıkılaştırma Tedbirleri
Windows İşletim Sistemi Sıkılaştırma Tedbirleri
Veri Tabanı Sıkılaştırma Tedbirleri
Genel Sıkılaştırma Tedbirleri
Sunucu Sıkılaştırma Tedbirleri
Web Sunucusu Sıkılaştırma Tedbirleri
Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

3.2. Rehber Uygulama Süreci

Şekil 1.'de görüldüğü gibi Rehber uygulama süreci, ISO/IEC 27001'de kullanılan "Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ)" modelindeki bilgi güvenliği yönetim sürecine benzemektedir. Rehber'in bu özelliği, hali hazırda Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulayan kurumlara rahatlıkla uygulanabilmesini sağlamaktadır.



Şekil 1. Bilgi ve İletişim Güvenliği Rehberi uygulama süreci (DDO, 2020)

4. ULUSLARARASI BİLGİ GÜVENLİĞİ STANDARTLARI

Bilgi ve İletişim Güvenliği Rehberi'nin hazırlanmasında aşağıda açıklamaları yapılan birçok uluslararası standart, kılavuz ve en iyi uygulamalardan yararlanılmıştır.

4.1. CMMC (Cybersecurity Maturity Model Certification)

Siber Güvenlik Olgunluk Modeli Sertifikasyonu olarak Türkçeye çevrilen CMMC, Amerika Birleşik Devletleri Savunma Bakanlığı'nın (DoD) Eylül 2020 yılında ilk versiyonunu yayımladığı, ulusal güvenliği ilgilendiren, bilgileri korumayı hedefleyen, savunma sanayiinde tedarikçi olarak çalışan ulusal ve uluslararası firmaların siber güvenlik olgunluklarını, belirli kriterlere göre ölçen ve bunu sertifikalandıran bir programdır (CMMC, 2021). Bilgi ve İletişim Güvenliği Rehberi'nde de "Ağ ve Sistem Güvenliği", "Taşınabilir Cihaz ve Ortam Güvenliği", "Personel Güvenliği", "Fiziksel Mekanların Güvenliği", "Kripto Uygulamaları Güvenliği", "Kritik Altyapılar Güvenliği" ve "Yeni Geliştirmeler ve Tedarik" güvenlik tedbirleri başlıklarında CMMC'de belirtilen kontrollerden yararlanılmıştır.

4.2. ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemi

ISO/IEC 27001, dünyada hemen hemen tüm sektörlerde en çok kullanılan bilgi güvenliği standardıdır. ISO/IEC 27001, kurum ve işletmelerin bilgi varlıklarını, Bilgi Güvenliği Yönetim Sistemi (BGYS) kurarak bilginin gizliliği, bütünlüğü ve erişilebilirliği özelliklerini korumayı amaçlayan ve bunu da risk yönetimi yaklaşımıyla gerçekleştiren uluslararası bir standarttır. BGYS'nin kurulması, işletilmesi, sürdürülmesi ve iyileştirilmesi için ISO/IEC 27001 ve ISO/IEC 27002 standartları birlikte kullanılmaktadır. ISO/IEC 27001 standardının Ek A bölümünde güvenlik denetimleri için kontrol maddeleri içermektedir (ISO/IEC 27001, 2017). Bilgi ve İletişim Güvenliği Rehberi'nde de sıkılaştırma tedbirleri hariç tüm varlık gruplarına yönelik hazırlanan güvenlik tedbirlerinde, ISO/IEC 27001 standardının etkisi görülmektedir. Ayrıca Dijital Dönüşüm Ofisi, "TS EN ISO/IEC 27001:2017 Kontrolleri ile Bilgi ve İletişim Güvenliği Rehberi Eşleştirme Tablosu" başlıklı bir doküman yayımlayarak kurumların, Rehber ve BGYS denetim süreçlerinin uyumlu olarak yönetilmesini desteklemektedir (DDO, 2021).

4.3. CIS Controls

CIS (Center for Internet Security), siber güvenlik alanında güven yaratma misyonuna sahip bağımsız, kar amacı gütmeyen, bilgi teknolojileri sistemlerini ve verilerini güvence altına almak için dünya çapında bilinen en iyi uygulamaları belirlemeye çalışan, küresel çapta bilişim teknolojileri uzmanları topluluğuna liderlik eden Amerika Birleşik Devletleri menşeli bir kuruluştur (CIS, 2021). CIS organizasyonu içinde oluşturulan CIS Controls ve CIS Benchmarks, en önemli iki siber güvenlik kılavuzu olup bunların yanında sistemlerin sıkılaştırılmış imajları da tüm dünyada ilgiyle takip edilen en iyi uygulamalardır. Bilgi ve İletişim Güvenliği Rehberi'nde yer alan tedbir seviyesi 1, 2, 3 yaklaşımı, CIS Controls yapısında uygulanan üç seviyeli koruma tedbir yaklaşımına benzemektedir. Rehberde, "Ağ ve Sistem Güvenliği", "Taşınabilir Cihaz ve Ortam Güvenliği", "Personel Güvenliği", "Kripto Uygulamaları Güvenliği", "Kritik Altyapılar Güvenliği" ve "Yeni Geliştirmeler ve Tedarik" güvenlik tedbirleri başlıklarında CIS Controls'da belirtilen güvenlik kontrollerinden yararlanılmıştır.

4.4. CIS Benchmark

CIS Benchmark'ları, sistemlerin güvenli yapılandırılması için en iyi yaklaşımı sunan bir kılavuzdur. CIS organizasyonu bünyesinde, 25 satıcı ürün ailesi içinden 100'den fazla oluşturulan CIS Benchmark'lar, dünya çapındaki bir çok siber güvenlik uzmanın katkılarıyla geliştirilmiştir.

CIS Benchmark'lar, hem kamu hem iş dünyası, hem de akademi tarafından geliştirilen en iyi uygulamaları barındıran güvenlik yapılandırma kılavuzlarıdır. CIS Benchmark dokümanlarında, işletim sistemleri, veri tabanları, sanallaştırma yazılımları ve ağ cihazları gibi birçok sistem hakkında oldukça fazla teknik detayın olduğu ve konu uzmanlarının ancak yorumlayabileceği sıkılaştırma önerileri bulunmaktadır. CIS Benchmark'lar, Rehber'de "İşletim Sistemi Sıkılaştırma", "Veri Tabanı Sıkılaştırma" ve "Sunucu Sıkılaştırma" tedbirlerinin hazırlanmasında önemli bir katkıya sahiptir.

4.5. Cloud Controls Matrix

Cloud Security Alliance (CSA), kar amacı gütmeyen, bulut bilişim güvenliği konusunda en iyi uygulamaların ve yaklaşımların belirlenmesinde rol alan, dünyanın bir çok yerinden gönüllü olarak çalışan uzmanların oluşturduğu bir organizasyondur (CSA, 2021). CSA'nın web sitesinde, bulut güvenliği konusunda oldukça fazla sayıda ücretsiz olarak elde edilebilen dokümanlar bulunmaktadır. Bunlardan biri de Rehber'de "Ağ ve Sistem Güvenliği", "Taşınabilir Cihaz ve Ortam Güvenliği", "Personel Güvenliği", "Fiziksel Mekanların Güvenliği", "Anlık Mesajlaşma Güvenliği", "Bulut Bilişim Güvenliği", "Kritik Altyapılar Güvenliği" ve "Yeni Geliştirmeler ve Tedarik" güvenlik tedbirleri başlıklarının oluşturulmasında etkisi olan Cloud Controls Matrix (CCM) çerçevesidir.

4.6. NIST 800-53

The National Institute of Standards and Technology (NIST) ABD Ticaret Bakanlığı bünyesinde çalışmalarını sürdüren Ulusal Standartlar ve Teknoloji Enstitüsü'dür. NIST, başta bilgi teknolojilerinde kullanılan sistemler olmak üzere birçok alanda ölçme faaliyetine yönelik metot ve standartları belirlemektedir. Özellikle NIST'in 800 serisinde yer alan dokümanlar, bilgi güvenliğinin konusu olan şifreleme standartları, taşınabilir cihaz güvenliği, bulut güvenliği, risk yönetimi, siber güvenlik çerçeveleri, politikaları ve prosedürleri tanımlamaktadır. NIST Special Publication 800-53 (NIST SP 800-53), "Security and Privacy Controls for Information Systems and Organizations" başlıklı bir doküman olup bilgi sistemleri ve kuruluşlar için güvenlik ve gizlilik kontrollerini içermektedir. NIST SP 800-53 Revision 5 dokümanında, 20 kontrol ana başlığı altında toplam 1.189 kontrol bulunmaktadır. Dokümandaki güvenlik ve gizlilik kontrolleri, sistemler, kuruluşlar ve bireyler için koruyucu önlemler sağlarken yasalara, düzenlemelere, politika ve standartlara uyumu kolaylaştırmak için tasarlanmıştır (NIST SP 800-53, 2020). Bilgi ve İletişim Güvenliği Rehberi gibi bir çok uluslararası organizasyon da standart, kılavuz, çerçeve ve metot gibi rehber niteliğindeki dokümanlar geliştirirken NIST'in en popüler dokümanlarından biri olan SP 800-53 ile uyumlu olmaya dikkat etmeye çalışmaktadır. Rehberde, "Ağ ve Sistem Güvenliği", "Taşınabilir Cihaz ve Ortam Güvenliği" ve "Kritik Altyapılar Güvenliği" güvenlik tedbirleri başlıklarının oluşturulmasında NIST SP 800-53 dokümanından yararlanılmıştır.

4.7. NIST 800-82

NIST SP 800-82 dokümanı "Guide to Industrial Control Systems (ICS) Security" adıyla 2015 yılında yayımlanmış olup SCADA, DCS ve PLC gibi endüstriyel kontrol sistemlerinin güvenliğine yönelik hazırlanmıştır (NIST SP 800-82, 2015). Dokümanda, Endüstriyel Kontrol Sistemlerinin (EKS) yapısı, güvenlik mimarisi ve topolojileri hakkında genel bir bilgi verilirken EKS sistemlerine yönelik tehdit ve güvenlik açıkları tanımlanarak ilişkili riskleri azaltmak için güvenlik tedbirleri önerilmektedir. NIST SP 800-82 dokümanda, EKS sistemleri için uygulanabilir güvenlik kontrollerinin birçoğu NIST SP 800-53'den seçilmiştir. Bununla birlikte dokümanda diğer NIST SP 800 serisinde yer alan ve endüstriyel kontrol sistemlerini ilgilendiren kontrollere de yer verilmiştir. Bilgi ve İletişim Güvenliği Rehberi'nde, "Kritik Altyapılar Güvenliği" tedbir maddelerinin hazırlanmasında NIST SP 800-82 dokümanından yararlanılmıştır.

4.8. NIST 800-125

NIST SP 800-125 dokümanı, "Guide to Security for Full Virtualization Technologies" adıyla 2011 yılında yayımlanmış olup sunucu ve masaüstü sanallaştırma için tam sanallaştırma teknolojileriyle ilişkili güvenlik endişelerini dile getirmekte ve bu endişeleri gidermek için de öneriler sunmaktadır. Dokümanda ayrıca sanallaştırma kavramlarının tanımı, sanallaştırma teknolojilerinin yapısı, özellikleri ve güvenlik önerilerine yer verilmektedir (NIST SP 800-125, 2011). Bilgi ve İletişim Güvenliği Rehberi'nde, sanal sunucu sıkılaştırmalarına yönelik tedbir maddelerinde NIST SP 800-125 dokümanında belirtilen güvenlik önerilerinden de yararlanılmıştır.

4.9. OWASP Application Security Verification Standard

OWASP (Open Web Application Security Project), yazılım güvenliği konusunda farkındalığı artırmak için bir çok araç, proje, teknik doküman ve metodoloji geliştiren, kar amacı gütmeyen uluslararası çevrimiçi bir topluluktur (Wikipedia, 2022). OWASP adını en çok web uygulama güvenliğine yönelik hazırlamış olduğu "Top 10" serisi ile duyurmuştur. OWASP Top 10 dokümanları, yazılım geliştiriciler ve uygulama güvenliği ile uğraşan uzmanlar için standart bir farkındalık belgesi olup siber güvenlik zafiyet ve tehditlerine vurgu yapmaktadır (OWASP, 2022). OWASP Application Security Verification Standard (ASVS), "Uygulama Güvenliği Doğrulama Standardı" olarak yazılım geliştiricilerin uygulamaları tasarlarken, geliştirirken ve test ederken dikkat etmesi gereken güvenlik kontrollerini içeren bir yapı sunmaktadır (OWASP, 2021). Rehber'de, "Uygulama ve Veri Güvenliği", "Kritik Altyapılar Güvenliği" tedbirler başlıklarının oluşturulmasında OWASP ASVS dokümanından yararlanılmıştır.

4.10. OWASP Mobile Application Security Verification Standard

OWASP Mobile Application Security Verification Standard (MASVS), Mobil Uygulama Güvenliği Doğrulama Standardı olarak 2017 yılında mobil uygulama güvenliği için hazırlanmış bir dokümandır (OWASP, 2022). Rehberde, "Uygulama ve Veri Güvenliği", "Taşınabilir Cihaz ve Ortam Güvenliği", "Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği" ve "Kritik Altyapılar Güvenliği" tedbirler başlıklarında OWASP MASVS dokümanından yararlanılmıştır.

4.11. OWASP IoT Security Verification Standard

OWASP IoT Security Verification Standard (ISVS), "IoT Güvenlik Doğrulama Standardı" olarak IoT uygulamaları için güvenlik gereksinimlerini belirler (OWASP, 2021). Bu belgede yer alan güvenlik gereksinimleri, IoT ekosistemi, kullanıcı uygulamaları, yazılım platformları, iletişim ve donanım platformları dahil olmak üzere IoT sistemleri ve uygulamalarının çeşitli yönlerini kapsamaktadır. Ayrıca dokümanda belirtilen güvenlik gereksinimleri, tasarım, geliştirme ve test dahil olmak üzere birçok ürün geliştirme aşaması için geçerlidir.

4.12. ENISA Security Aspects of Virtualization

2004 yılında kurulan European Network and Information Security Agency (ENISA), Avrupa Birliği (AB) siber güvenlik ajansıdır. Ajans, siber güvenlik yeteneklerini geliştirmenin yanı sıra tavsiye ve çözümler sunmak için AB üye devletleri ve diğer paydaşlarla yakın bir şekilde çalışmaktadır. ENISA, mevcut ve gelecekteki AB mevzuatı da dahil olmak üzere ağ ve bilgi güvenliği gereksinimlerini karşılamak için bir çok kılavuz, teknik doküman ve araştırma projeleri hazırlamaktadır. ENISA tarafından hazırlanan Sanallaştırmanın Güvenlik Yönleri (Security Aspects of Virtualization) raporunda ise sanallaştırma kavramlarından, sanallaştırma mimarisinin bileşenlerinden, sanallaştırma teknolojilerinin bilinen güvenlik açıklarından ve güvenlik

önlemlerinden bahsedilmektedir (ENISA, 2017). Rehber'de "Sunucu Sıkılaştırma" tedbirlerinin hazırlanmasında bu rapordan yararlanılmıştır.

4.13. DISA STIGs

Defense Information Systems Agency (DISA), asker, federal siviller ve tedarikçi firmalardan oluşan ABD Savunma Bakanlığı (DoD) muharebe destek kurumudur. DISA, ABD savunmasına katkıda bulunan herhangi bir kişi veya sisteme bilgi teknolojisi ve iletişim desteği sağlamak için yapmış olduğu birçok faaliyetin yanında referans dokümanlar, teknik kılavuzlar da hazırlamaktadır. Bu doküman serisinden biri de Security Technical Implementation Guides (STIGs), güvenlik teknik uygulama kılavuzlarıdır. Kılavuzlarda belirtilen güvenlik gereksinimleri, NIST 800-53 ve ilgili belgelerden türetilmiştir. STIG dokümanları özellikle ağ ve sistem sunucuları, veri tabanları, güvenlik duvarları gibi birçok ürünün sıkılaştırmasında kullanılmaktadır (STIG, 2022).

Rehber'de "Linux İşletim Sistemi Sıkılaştırma" tedbirlerinin hazırlanmasında "DISA STIG - Canonical Ubuntu 16.04 LTS Security Technical Implementation Guide", "DISA STIG - Red Hat Enterprise Linux 7 Security Technical Implementation Guide", "Red Hat Enterprise Linux 8 Security Hardening", "Ubuntu Server Guide – Security" ve "Oracle Linux 7 Security Guide" dokümanlarından da yararlanılmıştır.

5. NESNELERİN İNTERNETİ (IoT) GÜVENLİĞİ

IoT cihazlarının mimari yapısı ve kullandığı iletişim protokolleri gereği bazı kısıtları bulunmaktadır. Sınırlı işlem gücü, sınırlı veri depolama kapasitesi, veri iletiminde sınırlı bant genişliği , sınırlı güç tüketimi ve düşük veri iletim hızı gibi teknik kısıtlar saldırganlar için de birer saldırı yüzeyi oluşturmaktadır (Asma vd., 2016) IoT saldırı vektörlerinin kök nedenlerinden biri de IoT cihaz üreticilerinin rekabet üstünlüğü elde etmek için güvenli tasarım ilkesini dikkate almadan hızlı ürün çıkarmalarıdır. Farklı IoT ürünlerinin varlığı, geliştirme süreçlerinde güvenlik alanında bilgi birikimini oluşmasını da yavaşlatmaktadır. Cihazlara yönelik güvenlik sorunları çıktığında da genellikle geçici çözümler üretilmekte ve saldırıların kök nedeni bulunamamaktadır.

Tablo 4.'de OWASP IoT Top 10 listesi görülmektedir. IoT sistemlerindeki zafiyetlere dikkat çekmek amacıyla hazırlanan bu liste dikkatlice incelendiğinde basit önlemler alınarak bile IoT cihazlarında belirli seviyede güvenliği sağlamanın mümkün olabileceği görülebilmektedir.

Tablo 4. OWASP IoT Top 10

1	Zayıf, Tahmin edilebilir veya Sabit Kodlanmış Parolalar
2	Güvensiz Ağ Servisleri
3	Güvensiz Ekosistem Ara yüzleri
4	Güvenli Güncelleme Mekanizmasının Eksikliği
5	Güvensiz veya Kullanımdan Kaldırılmış Bileşenler
6	Yetersiz Mahremiyeti Koruma Tedbirleri
7	Güvensiz Veri Transferi ve Depolaması
8	Cihaz Yönetimi Eksikliği
9	Güvensiz Varsayılan Ayarlar
10	Fiziksel Sıkılaştırma Eksikliği

IoT güvenliğinden söz edebilmek için IoT sistemindeki uçtan uca bütün bileşenlerin güvenlik unsurları dikkatle ele alınmalıdır. Sensörler, kontrolörler, ağ ve güvenlik cihazları, donanım cihazları, hücresel, kablolu ve kablosuz iletişim ortamları, mobil uygulamalar, web uygulamaları, bulut servisleri gibi verinin elde edildiği, iletiminin yapıldığı, saklandığı ve işlendiği tüm ortamlar güvenli bir IoT sistemi için risk çalışmasına dahil edilmeli ve bu riskleri azaltmaya yönelik güvenlik önlemleri hayata geçirilmelidir. IoT sistemlerine yönelik alınması gereken güvenlik önlemleri, "Ağ Güvenliği" , "İletişim Güvenliği", "Veri Güvenliği", "Cihaz Güvenliği", "Bulut ve Uygulama Güvenliği", "Kimlik Doğrulama ve Yetkilendirme", "İşletim Güvenliği" ve "Uyum, Risk Yönetimi, Farkındalık, Güvenlik Testleri" başlıkları altında incelenebilir.

6. IoT GÜVENLİĞİ İÇİN BİR UYGULAMA ÖRNEĞİ

Ulusal Bilgi ve İletişim Güvenliği Rehberi'nde varlık gruplarına yönelik 661 güvenlik tedbirine yer verilmiştir. Bu çalışmada, Rehber'in tedbir maddelerindeki güvenlik yaklaşımının daha iyi anlaşılması için kapsam daraltması yapılarak sadece Rehber ana başlıklardan biri olan IoT güvenliğine yönelik tedbirler detaylı olarak incelenmiştir. Bununla birlikte çalışmanın amaçlarından biri de IoT ortamlarının güvenliğinin nasıl sağlanabileceğine dair bir uygulama platformu oluşturmaktır. Özellikle IoT sistemleri için test ortamı oluşturma maliyetinin yüksek olması ve aktif çalışan IoT ortamında güvenlik denetimlerinin yapmanın yüksek risk barındırması sebebiyle simülasyon ortamına ihtiyaç bulunmaktadır. Bu çalışmada da Cisco Packet Tracer kullanılarak simülasyon ortamı oluşturulmuş ve Rehberdeki IoT güvenliğine yönelik tedbirlerin, temsili kurumun yapısıyla uyumlu olup olmadığı kontrol edilmiştir.

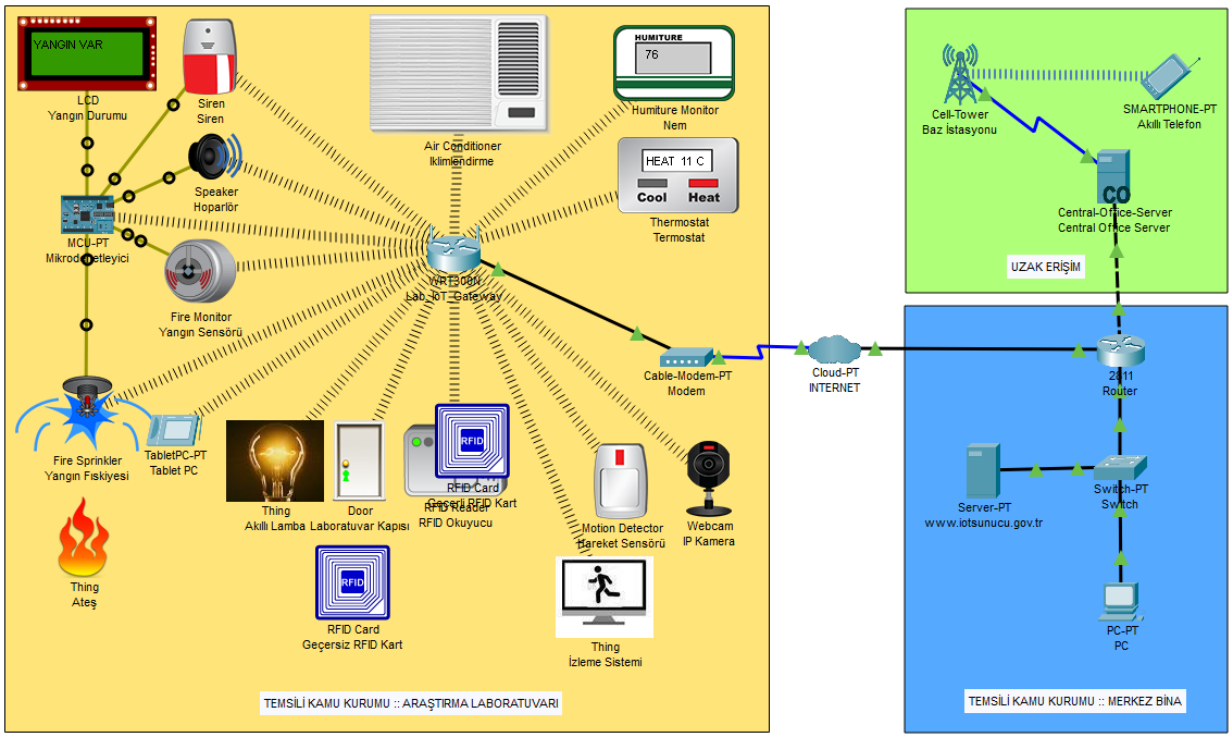
6.1. Temsili Kurumun IoT Simülasyon Ortamı

Temsili kurumunun IoT simülasyon ortamı Packet Tracer aracı kullanılarak oluşturulmuştur (Şekil 2.). Cisco tarafından geliştirilen Packet Tracer yazılımı, kullanıcıların ağ, siber güvenlik ve IoT konusunda yetkinliklerini geliştirmelerine imkan veren bir ağ simülasyon ve görselleştirme aracıdır (Cisco, 2022).

Bu çalışma için örnek teşkil eden temsili kurum, AR-GE faaliyetlerinde bulunan ve bir araştırma laboratuvarına sahip kamu kurumudur. Temsili kamu kurumunun merkez binası il merkezinde bulunurken araştırma laboratuvarı ise ilçe merkezindedir. Araştırma laboratuvarının güvenliği için IoT sensörler yerleştirilmiş ve bunların çalışması ve ürettiği alarmlar izlenmektedir. Sensörlerin ve IoT sisteminin yönetimi il merkez binasında bulunan IoT sunucu tarafından yönetilmektedir. Ayrıca IoT cihazlarının durumu uzaktan akıllı telefon yardımı ile de izlenebilmektedir. Tablo 5.'de temsili kurumun laboratuvarında kullandığı IoT cihazları görülmektedir.

Tablo 5. Temsili kurumun laboratuvar ortamında kullandığı IoT cihazları

Laboratuvar IoT Cihazları
Nem Sensörü
Sıcaklık Sensörü (Termostat)
İklimlendirme
Yangın Sistemi (Yangın Sensörü, Alarm Sistemi, Yangın Fıskiyesi)
RFID Okuyucu – RFID Kart
Hareket Sensörü
IP Kamera
Akıllı Lamba
Mikrodenetleyici
IoT Gateway
IoT Sunucu



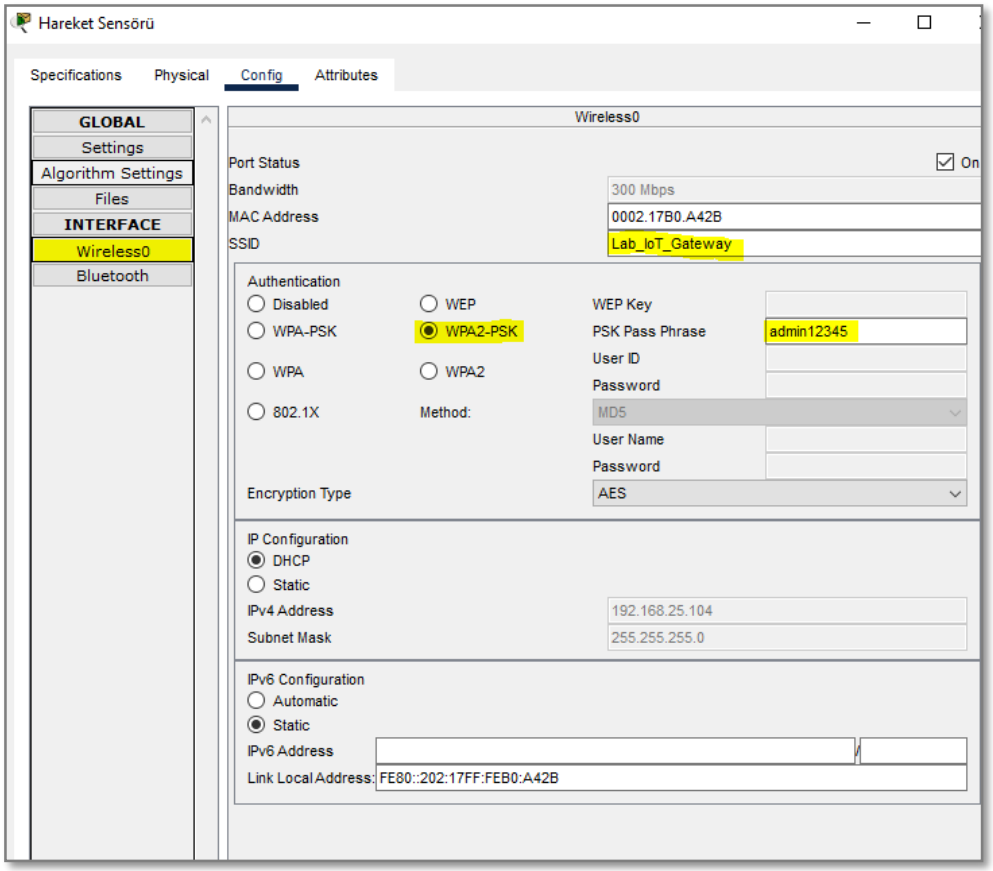
Şekil 2. Temsili kurumun IoT simülasyon ortamı

Şekil 2.'de gösterilen simülasyon ortamı, temsili kamu kurumuna ait IoT topolojisidir. Topolojinin çalışması için gerekli olan modem, yönlendirici, anahtar gibi ağ cihazlarının yapılandırma ayarlarına burada değinilmeyip simülasyon üzerinde gerekli ayarlar yapılmıştır. Tablo 6.'de ise araştırma laboratuvarına konumlandıran IoT cihazlarının kullanım amaçları belirtilmektedir.

Tablo 6. Temsili kurumun IoT cihazlarının kullanım amaçları

IoT Cihazı	Kullanım Amacı
Yangın Sensörü, Yangın Fıskiyesi, Siren, Hoparlör, LCD Ekran, Mikrodenetleyici, IoT Gateway, IoT Sunucu	Yangın çıktığında yangın alarm sistemini devreye sokarak ses ve görsel bildirimde bulunmak
RFID Okuyucu, RFID Kart, Akıllı Lamba, Kapı, IoT Gateway, IoT Sunucu	Geçerli RFID kartını okuyarak yetkili kişilere laboratuvar kapısını açmak ve ortamı aydınlatmak
Hareket Sensörü, IP Kamera, İzleme Sistemi, IoT Gateway, IoT Sunucu	Laboratuvar kapı girişinde hareket olduğunda kamera ile ortamın fotoğrafını çekip IoT sunucusuna göndermek
Nem Sensörü, İklimlendirme, Sıcaklık Sensörü, IoT Gateway, IoT Sunucu	Laboratuvar ortamının sıcaklık ve nem değerlerine göre iklimlendirme cihazını çalıştırmak

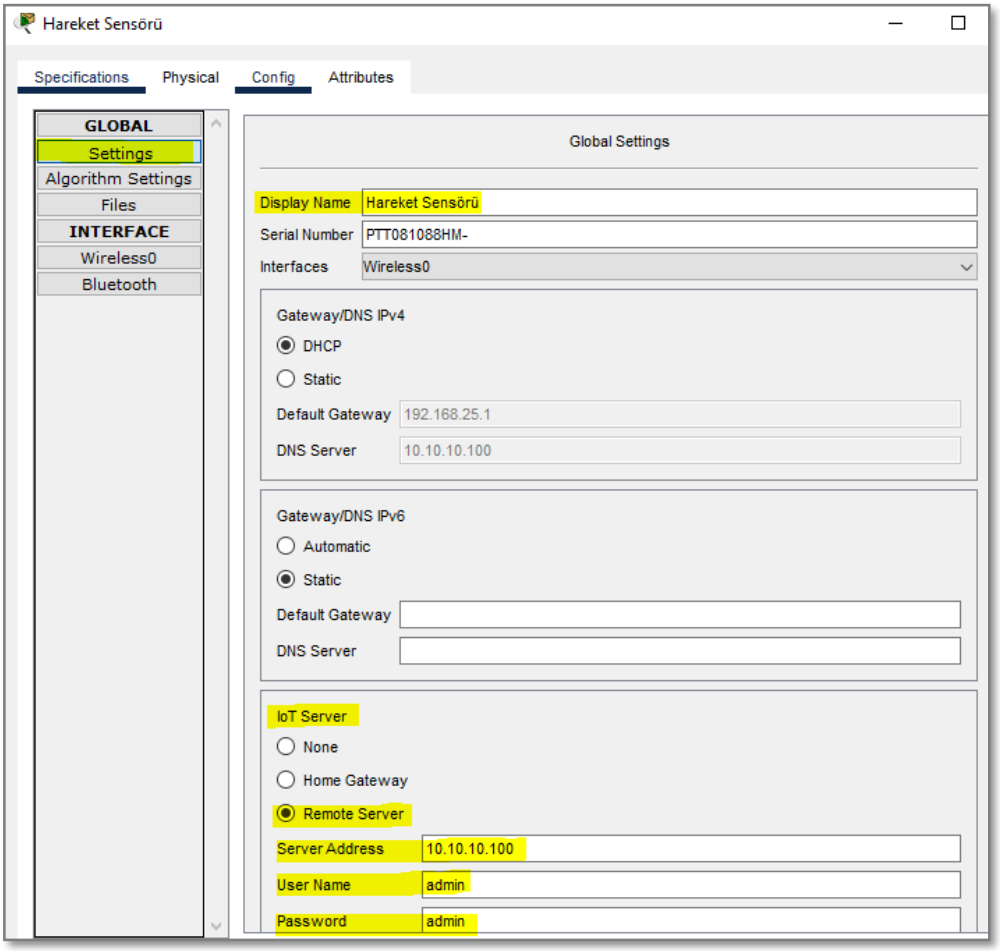
Sensörlerin ve mikrodenetleyicilerin çalışır hale getirilmesinden sonra bunların IoT Gateway ile iletişim kurması için yapılandırma ayarlarının yapılması gerekmektedir. Şekil 3.'de hareket sensörünün IoT gateway ile kablosuz erişim yapılandırmasında kullanılan ekranı görülmektedir. Şekil 3.'deki gibi tüm sensörler kablosuz iletişimde SSID olarak "Lab_IoT_Gateway" adını, kimlik doğrulama için "WPA2-PSK" protokolünü ve şifreleme için "AES" algoritmasını kullanmaktadır.



Şekil 3. Hareket sensörünün IoT gateway ile kablosuz erişim yapılandırması

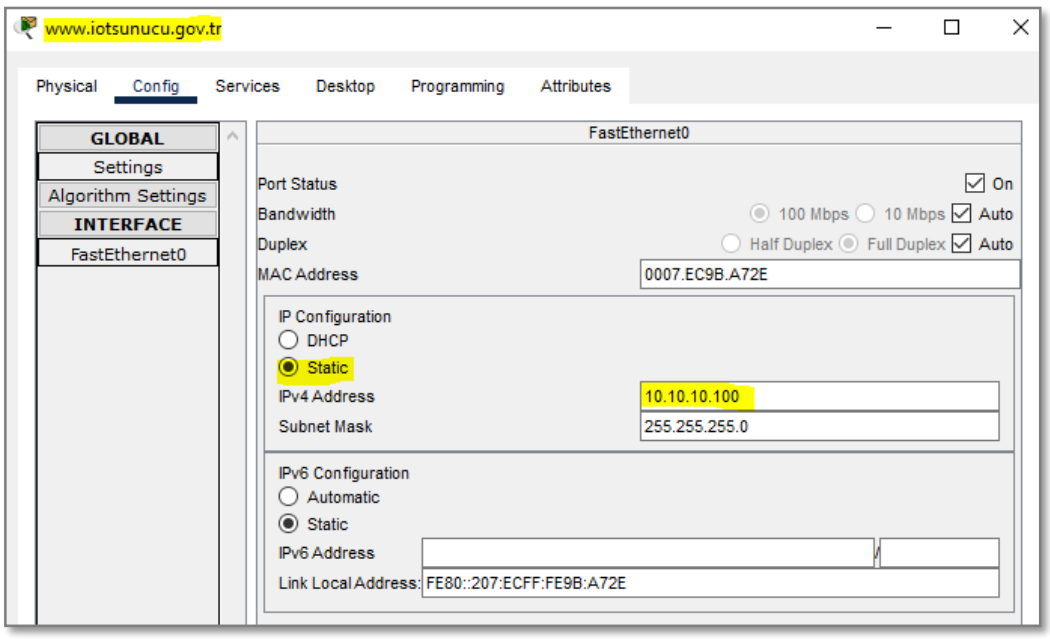
Hareket sensörünün IoT sunucusuna veri gönderebilmesi için Şekil 4.'deki ekranda olduğu gibi IoT Server sekmesine sunucu IP adresi, kullanıcı adı ve parola bilgilerinin girilmesi gerekmektedir. Bu bilgilerin aynı şekilde tüm sensör ve akıllı cihazların yapılandırma ayarlarına girilmesi gerekmektedir.

Burada kullanıcı adı ve parolaların varsayılan kullanıcı adı ve parola olarak kullanıldığı, IoT sunucusunun DNS Server olarak yapılandırıldığı ve IP adreslerinin DHCP servisi ile otomatik olarak dağıtıldığı görülmektedir. Ayrıca tüm IoT cihazlarının IoT Gateway ile iletişim kurabilmesi için aynı kablosuz ağ içinde bulunması gerekmektedir.



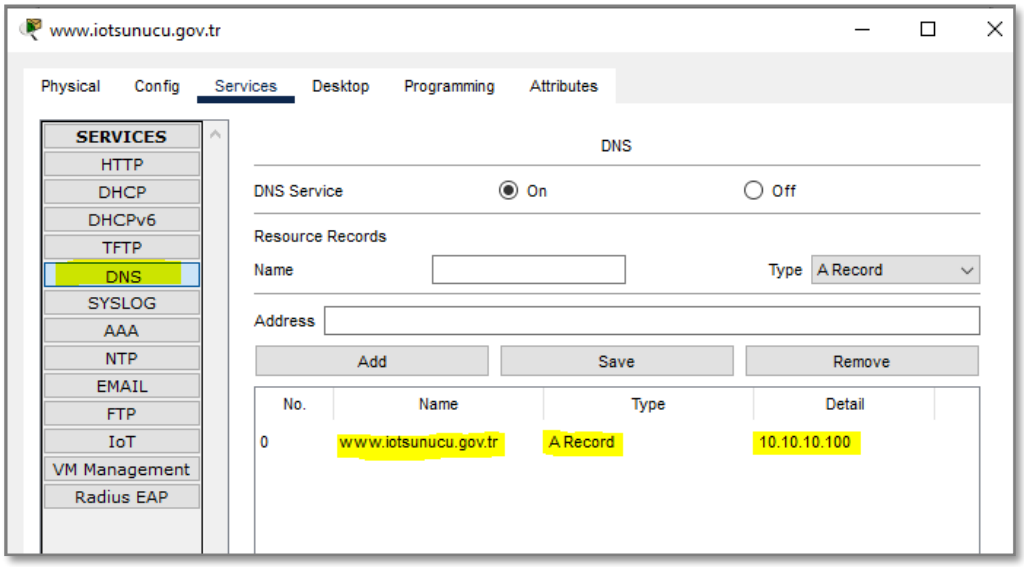
Şekil 4. Hareket sersörünün IoT sunucu ile kimlik doğrulama yapılandırması

IoT gateway, sensörlerdeki verinin uzak noktalardaki uygulama sunucularına gönderilmesi ve alınmasında köprü görevi görmektedir. Gateway üzerindeki yapılandırmalar sistemin güvenliği için büyük önem arz etmektedir. IoT sunucusunda kayıtlı tüm akıllı nesneler, bir bilgisayar veya akıllı telefon kullanılarak bir web ara yüzü üzerinden uzaktan erişilerek kontrol edilebilmektedir. Bu nedenle, tüm akıllı cihazların aynı IP adresini kullanarak IoT sunucusuna bağlanabilmesi için Şekil 5.'deki gibi IoT sunucusunun statik bir IP adresi ile yapılandırılması gerekmektedir.



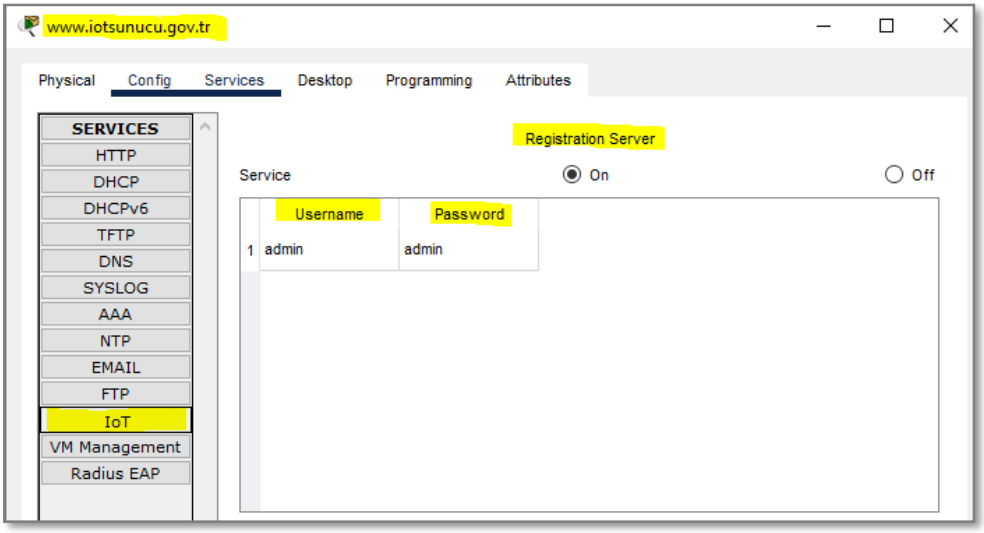
Şekil 5. IoT sunucusunun statik IP adresi yapılandırması

Kullanıcıların, IoT sunucusuna uzaktan erişiminde IP adresi yerine Şekil 6.'da görüldüğü gibi "www.iotsunucu.gov.tr" alan adını kullanarak erişmesini sağlamak için de IoT sunucusu aynı zamanda DNS sunucusu olarak yapılandırılması gerekmektedir.



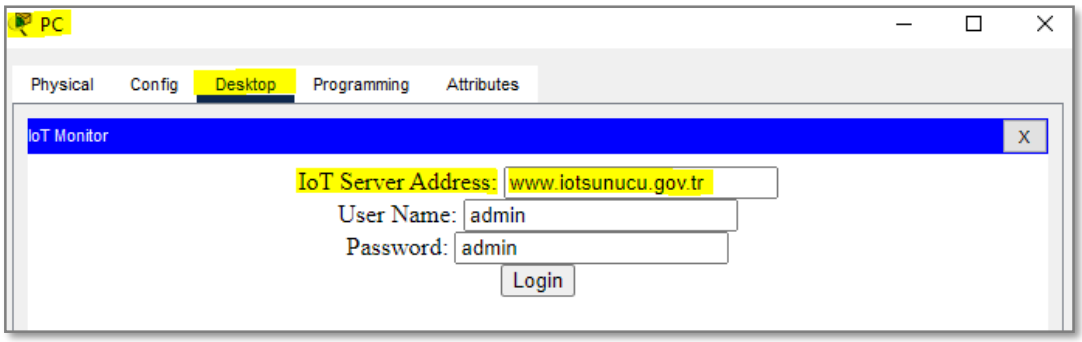
Şekil 6. IoT sunucusunun DNS yapılandırması

Şekil 7.'de ise tüm IoT cihazlarının IoT sunucusuna kaydolabilmesi için sunucu kimlik doğrulamada gerekli olan kullanıcı adı ve parola bilgilerinin tanımlandığı ekran görülmektedir. Bu bilgilerin kurum erişim ve parola politikalarına uygun bir şekilde tanımlanması olası siber güvenlik risklerini azaltacaktır.



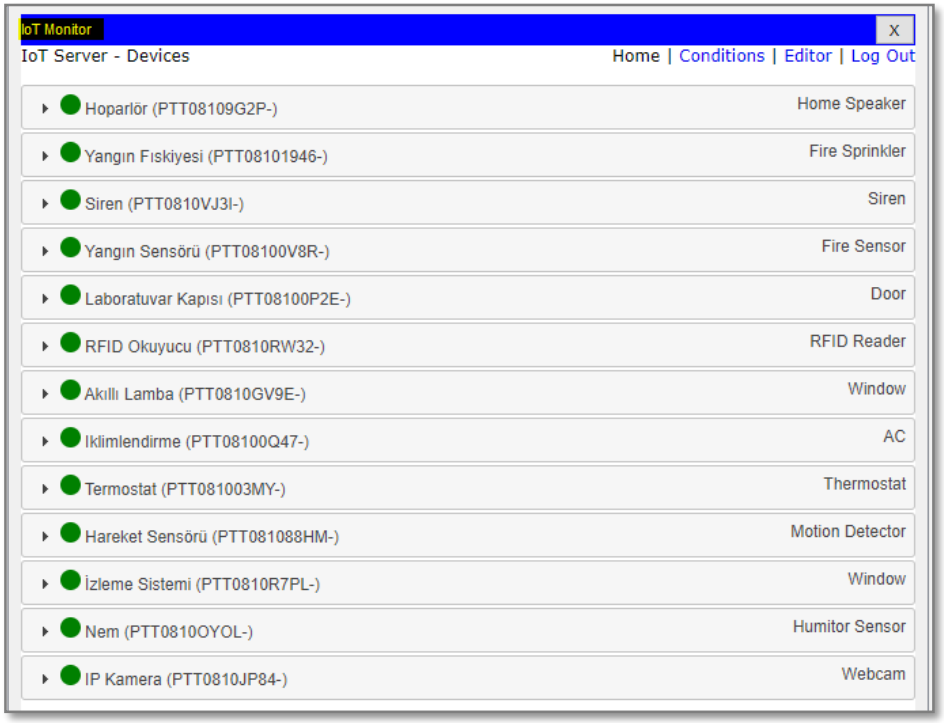
Şekil 7. IoT sunucusunun kimlik doğrulama yapılandırması

Şekil 8.'de ise kurum ağındaki bir bilgisayardan IoT sunucusuna bağlanmaya çalışıldığı görülmektedir. IoT sunucusu oturum açma ekranında sunucu adresi, kullanıcı adı ve parola bilgileri girilerek kullanıcının kimlik doğrulaması yapılmaktadır.



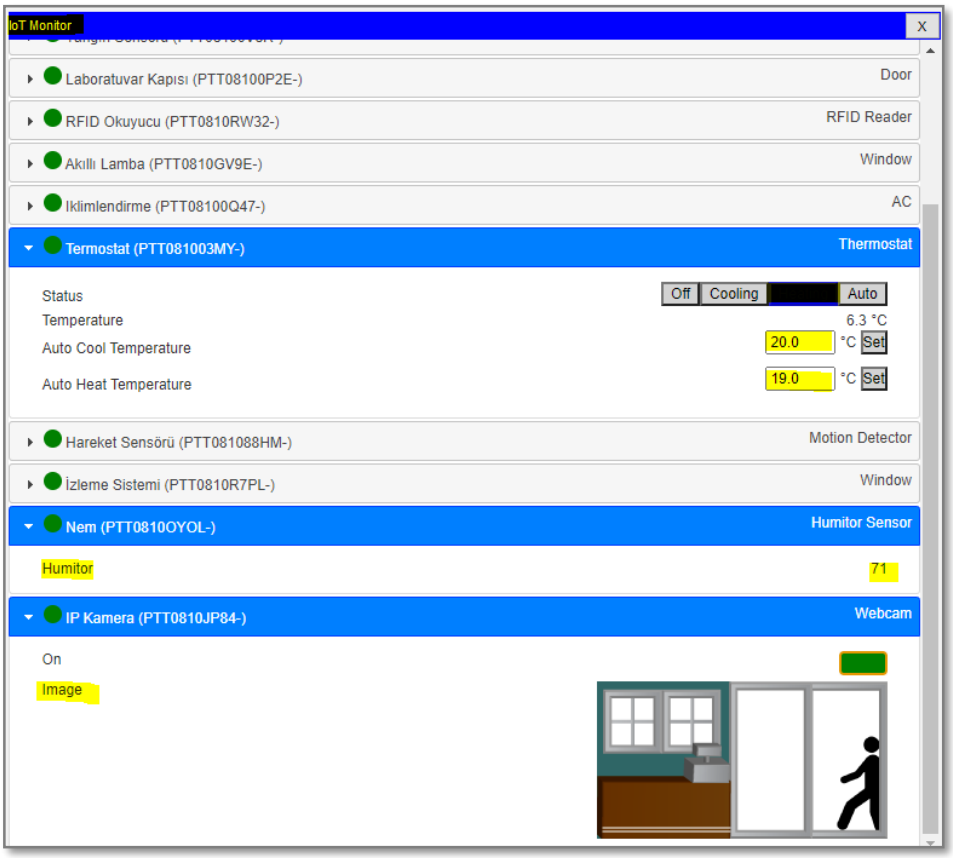
Şekil 8. IoT sunucusu oturum açma ekranı

IoT sunucusuna yapılan başarılı oturum açma işlemi sonrasında Şekil 9.'daki gibi IoT sunucusuna kayıtlı cihazlar görülmektedir.



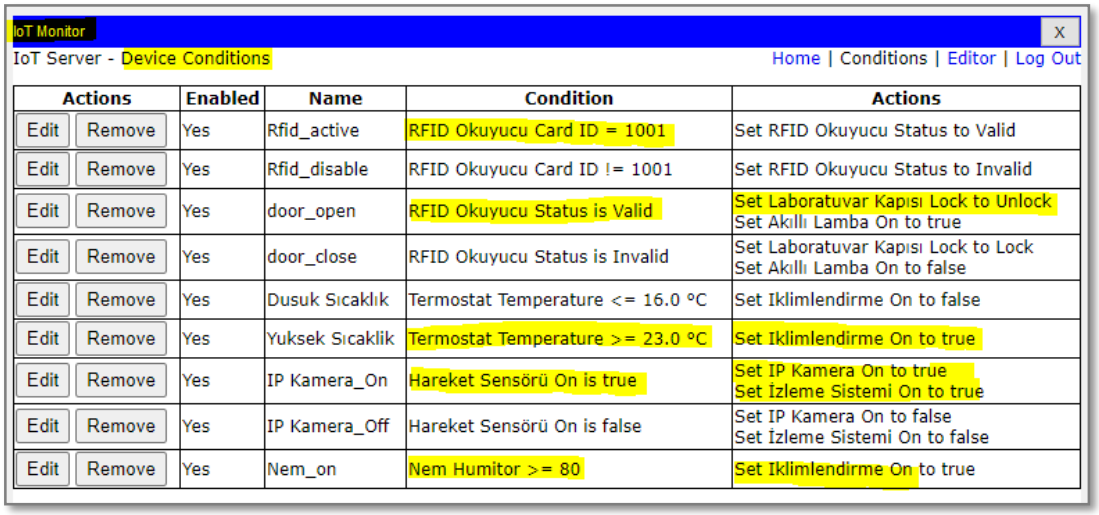
Şekil 9. IoT sunucusuna kayıtlı cihazlar

Bu cihazların yönetimi yine bu ara yüz üzerinden yapılabilmektedir (Şekil 10.).



Şekil 10. IoT sunucusuna bağlı cihazların yönetimi

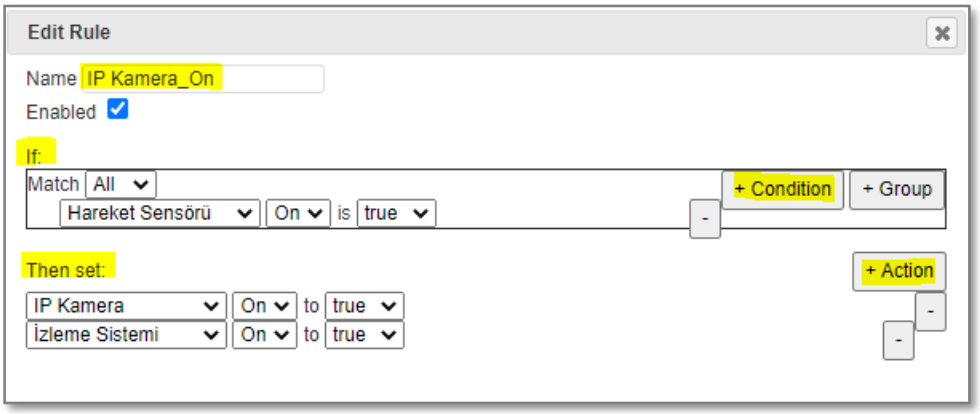
Şekil 11.'de görülen IoT sunucusunun "Conditions" sekmesi kullanılarak IoT cihazlarının belirli şartlar altında nasıl davranacağı da belirlenebilmektedir.



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Rfid_active	RFID Okuyucu Card ID = 1001	Set RFID Okuyucu Status to Valid
Edit Remove	Yes	Rfid_disable	RFID Okuyucu Card ID != 1001	Set RFID Okuyucu Status to Invalid
Edit Remove	Yes	door_open	RFID Okuyucu Status is Valid	Set Laboratuvar Kapısı Lock to Unlock Set Akıllı Lamba On to true
Edit Remove	Yes	door_close	RFID Okuyucu Status is Invalid	Set Laboratuvar Kapısı Lock to Lock Set Akıllı Lamba On to false
Edit Remove	Yes	Dusuk Sıcaklık	Termostat Temperature <= 16.0 °C	Set Iklimlendirme On to false
Edit Remove	Yes	Yuksek Sıcaklik	Termostat Temperature >= 23.0 °C	Set Iklimlendirme On to true
Edit Remove	Yes	IP Kamera_On	Hareket Sensörü On is true	Set IP Kamera On to true Set İzleme Sistemi On to true
Edit Remove	Yes	IP Kamera_Off	Hareket Sensörü On is false	Set IP Kamera On to false Set İzleme Sistemi On to false
Edit Remove	Yes	Nem_on	Nem Humitor >= 80	Set Iklimlendirme On to true

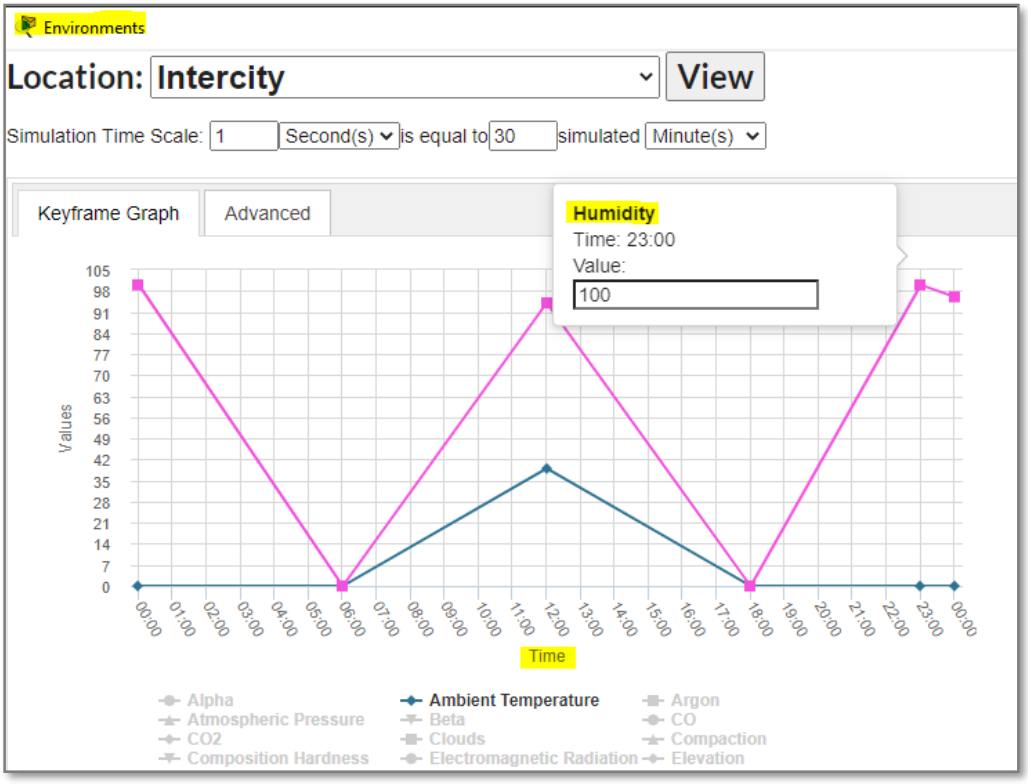
Şekil 11. IoT sunucusuna bağlı cihazların durumsal koşullara göre hareketi

Örneğin, Şekil 12.'de belirtilen kurala göre eğer Hareket Sensörünün "On" değeri "true" değerine sahip olursa IP Kamera ve İzleme Sisteminin de "On" değeri true olacaktır. Böylece hareket sensörü, herhangi bir nesnenin hareketini algılayarak IP kamerayı tetikleyecek ve kamerada ortamdaki hareketin fotoğrafını çekerek İzleme Sistemine gönderecektir.



Şekil 12. IoT sunucusuna bağlı hareket Sensörüne yönelik hazırlanan kural

Cisco Packet Tracer yazılımı ile ışık, duman, nem, karbondioksit, sıcaklık, yerçekimi gibi çevresel koşullar simüle edilebilmektedir. Bir çok IoT cihazı da bir şekilde çevresel koşullarla etkileşime girerek ortamı etkilemektedir. Şekil 13.'de ise IoT sisteminin bulunduğu çevresel koşulların ayarlandığı Packet Tracer yazılımının "Environments" ekranı görünmektedir. Bu ekranda 24 saatlik çevresel koşullar simüle edilmektedir. Bu çalışmadaki simülasyon ortamında ise her 1 saniye 30 dakikalık zamanı temsil etmektedir.



Şekil 13. IoT sisteminin bulunduğu çevresel koşullar

6.2. Temsili Kurumun Rehber IoT Güvenliği Uyumunun Değerlendirilmesi

Temsili kurumun Rehber IoT güvenliği uyumunun değerlendirilmesi için Şekil 2.'de oluşturulan IoT simülasyon ortamı esas alınmaktadır. Temsili kurumun Rehber uyumunda şu beş ana madde üzerinden değerlendirmesi yapılacaktır:

1. IoT varlık gruplarının belirlenmesi
2. IoT varlık gruplarının kritiklik derecelerinin belirlenmesi
3. IoT varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi
4. IoT varlık gruplarının mevcut durum ve boşluk analizi çalışmasının yapılması
5. IoT varlık gruplarına yönelik uygulama yol haritasının oluşturulması

6.2.1. IoT varlık gruplarının belirlenmesi

Bu çalışmanın kapsamı Rehber IoT güvenliği ile sınırlandırıldığı için varlık gruplarının belirlenmesinde de sadece IoT cihazları dikkate alınmıştır. IoT cihazlarının iletişim kurması için gerekli olan ağ ve sistem cihazları bu varlık gruplarına dahil edilmemiştir. Nem, sıcaklık ve hareket sensörleri ile iklimlendirme ve akıllı lamba ortak işlevlere sahip oldukları düşünülerek tek bir varlık grubu altında toplanmıştır. Yangın sensörü, alarm sistemi ve yangın fiskiyesi de aynı ortak amaca hizmet ettikleri için "Yangın Sistemi" varlık grubu başlığı altına alınmıştır (Tablo 7.).

Tablo 7. IoT varlık grupları

Varlık Grubu Ana Başlığı	Varlık Grubu No	Varlık Grubu Adı
Nesnelerin İnterneti (IoT) Cihazları	3.4.1	IP Kamera
	3.4.2	Sensörler - İklimlendirme - Akıllı Lamba
	3.4.3	Yangın Sistemi
	3.4.4	RFID Okuyucu – RFID Kart
	3.4.5	Mikrodenetleyici
	3.4.6	IoT Gateway
	3.4.7	IoT Sunucu

6.2.2. IoT varlık gruplarının kritiklik derecelerinin belirlenmesi

IoT varlık gruplarının kritiklik derecelerini belirlemek için Rehber'de EK-C.1'de yer alan "Varlık Grubu Kritiklik Derecelendirme Anketi'nin" doldurulması gerekmektedir. Bu nedenle varlık sahipleri, sistem yöneticileri ve teknik uzmanlardan oluşan 5 kişilik bir çalışma grubu oluşturularak Tablo 7.'de belirtilen her varlık grubu için kritiklik derecesi belirlenmiştir.

Şekil 14.'de Sensörler varlık grubuna yönelik hazırlanmış olan kritiklik derecesi belirleme anketi görülmektedir. Benzer çalışma diğer IoT varlık grupları için de yapılmış olup tüm IoT varlık gruplarının kritiklik derecesi 1 olarak tespit edilmiştir.

Varlık Grubu: 3.4.2. Sensörler- İklimlendirme- Akıllı Lamba

Boyut	Soru No.	Şıkların Puanları					Soru Puanı
		a	b	c	d	e	
İşlenen Veri Açısından							
Gizlilik	1	1 puan	2 puan	3 puan	5 puan		1
Bütünlük	2	1 puan	2 puan	3 puan	5 puan		1
Erişilebilirlik	3	1 puan	2 puan	3 puan	5 puan		1
Etki Alanı Açısından							
Etkilenen Kişi Sayısı	4	1 puan	2 puan	3 puan	4 puan	5 puan	1
Toplumsal Sonuçlar	5	1 puan	2 puan	3 puan	5 puan	6 puan	1
Kurumsal Sonuçlar	6	1 puan	2 puan	3 puan			1
Sektörel Etki	7	1 puan	2 puan	3 puan	5 puan		1
Bağımlı Varlıklar	8	1 puan	2 puan	3 puan	5 puan	6 puan	1
Anket Puanı (Tüm soruların puanlarının toplamı)							**8**
Varlık Grubu Kritiklik Derecesi							**Derece 1**

Şekil 14. Sensörler varlık grubunun kritiklik derecesi belirleme anketi

6.2.3. IoT varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi

Bu çalışmada oluşturulan temsili kurumun sahip olduğu tüm IoT varlık gruplarının kritiklik derecesi 1 olduğu için Rehber'deki güvenlik tedbirlerinden sadece 1. seviye tedbirlerin seçilmesi gerekmektedir. Ayrıca Şekil 15.'de görüldüğü gibi IoT varlık gruplarına yönelik hangi 1.

seviyedeki tedbir maddelerinin uygulanabilir olduğunu belirlemek için Rehber'de yer alan "Varlık Gruplarına Yönelik Güvenlik Tedbirleri", "Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri" ve "Sıkılaştırma Faaliyetlerine Yönelik Güvenlik Tedbirleri" ana başlıklarındaki tedbir maddelerinin gözden geçirilmesi gerekmektedir.

TEMSİLİ KAMU KURUMU
VARLIK GRUBU VE KRİTİKLİK DERECESİ TANIMLAMA FORMU

Varlık Grubu Ana Başlığı	Varlık Grubu No	VarlıkGrubuAdı	Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri (Her varlık grubu için aşağıdaki başlıkların Uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)						Sıkılaştırma Tedbirleri (Her varlık grubu için aşağıdaki başlıkların Uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)			Kritiklik Derecesi (Derece 1 / Derece 2 / Derece 3)
			Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik	İşletim Sistemi Sıkılaştırma Tedbirleri	Veri Tabanı Sıkılaştırma Tedbirleri	Sunucu Sıkılaştırma Tedbirleri	
Nesnelerin İnterneti (IoT) Cihazları	3.4.1	IP Kamera	U	UD	UD	UD	UD	UD	UD	UD	UD	Derece 1
	3.4.2	Sensörler- Akıllı Klima- Akıllı Lamba	UD	UD	UD	UD	UD	UD	UD	UD	UD	Derece 1
	3.4.3	Yangın Sistemi	UD	UD	UD	UD	UD	UD	UD	UD	UD	Derece 1
	3.4.4	RFID Okuyucu – RFID Kart	UD	UD	UD	UD	UD	UD	UD	UD	UD	Derece 1
	3.4.5	Mikrodenetleyici	UD	UD	UD	UD	UD	UD	UD	UD	UD	Derece 1
	3.4.6	IoT Gateway	UD	UD	UD	UD	UD	UD	UD	UD	UD	Derece 1
	3.4.7	IoT Sunucu	U	UD	UD	UD	UD	UD	U	UD	U	Derece 1

Şekil 15. Varlık gruplarına yönelik tedbirlerin uygulanabilirliği

Örneğin Sensörler varlık grubu için Şekil 15.'e bakıldığında "Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri" ve "Sıkılaştırma Faaliyetlerine Yönelik Güvenlik Tedbirleri" ana başlıklarındaki tedbir maddelerinin hiç birinin uygulanabilir olmadığı görülmektedir. Bu nedenle Sensörler varlık grubu için sadece "Varlık Gruplarına Yönelik Güvenlik Tedbirleri" ana başlığındaki 1. Seviye tedbir maddelerinden uygulanabilir olanlar seçilmelidir.

6.2.4. IoT varlık gruplarının mevcut durum ve boşluk analizi çalışmasının yapılması

Şekil 15.'e göre oluşturulan IoT varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi ile temsili kamu kurumunun IoT varlık grupları için mevcut durum ve boşluk analizi çalışması yapılabilmektedir. Tablo 6.'da belirtilen her bir IoT varlık grubu için uygulanabilir olan 1. seviyedeki tedbir maddelerine bakılarak kurumun Rehber IoT güvenliği kapsamında hangi oranda uyumlu olduğu mevcut durum ve boşluk analizi çalışmasıyla ortaya çıkarılmaktadır. Bu çalışmada uygulanabilir tedbir maddelerinin oldukça fazla olması ve her bir tedbir maddesinin de tüm IoT varlık grupları için de uygulanması gerekliliğinden dolayı örneklem seçimine gidilmiştir. Burada mevcut durum ve boşluk analizi çalışması sadece "IoT Sunucu" varlık grubu için ve sadece "Varlık Gruplarına Yönelik Güvenlik Tedbirleri" ana başlığı altındaki "Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği" tedbir maddeleri seçilerek yapılmıştır (Tablo 8.).

Tablo 8. IoT cihazlarının güvenliğine yönelik 1. seviye tedbirler (DDO, 2020)

3.4. Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği			
3.4.1. Ağ Servisleri ve İletişimi			
Tedbir No	**Tedbir Seviyesi**	**Tedbir Adı**	**Tedbir Tanımı**
3.4.1.1	1	Ağ Portlarının Kısıtlanması	Cihazlarda sadece ilgili fiziksel ve mantıksal portlar ile servisler açık bırakılmalıdır.
3.4.1.2	1	Ağ Servislerinin Güvenlik Kontrolleri	Gerekli tüm ağ servislerinin açıklara ve saldırılara karşı kontrolleri periyodik olarak yapılmalıdır.
3.4.1.3	1	Güvenli Yapılandırma	Cihaza yönelik aşağıda yer alan işlemlerin yapılması ve işlemler sırasında gerekli tüm bilgilerin güvenli bir şekilde aktarılması sağlanmalıdır. Cihaz kurulumu Konfigürasyon güncellemeleri Sistem yazılımı güncellemeleri İşletim sistemi ve kütüphane güncellemeleri IoT cihazlarının kurulumu ve yapılandırılması, yeniden başlatma ve kurtarma işlemleri vb. operasyonel ve yönetsel faaliyetlere ilişkin işletim prosedürleri hazırlanmalıdır.
3.4.1.4	1	Cihazın Güvenli İmhası veya Tekrar Kullanımı	Cihazın depolama ortamı içeren tüm parçaları elden çıkarılmadan veya yeniden kullanılmadan önce, herhangi bir kritik veri ve/veya lisanslı yazılım varsa kaldırılmasını veya güvenli şekilde üzerine yazılmasını sağlamak için kontrol edilmelidir. Verinin ve veri içeren ortamların güvenli imhası için işletilecek yöntemler verinin kritikliği göz önünde bulundurularak sınıflandırılmalı, yazılı hale getirilmeli ve uygulamaya alınmalıdır.
3.4.1.5	1	Yetkisiz Cihazların Kurum Ağına Bağlanmasının Engellenmesi	IoT cihazlarının izin alınmadan ağa bağlanmalarını ve yer değiştirmelerini engellemek amacıyla gerekli önlemler alınmalıdır.
3.4.2. Dâhili Veri Depolama			
3.4.2.1	1	Veri Yedekleme	Cihaz üzerinde yer alan veri, bilgi güvenliği ve yedekleme ihtiyaçları doğrultusunda düzenli olarak yedeklenmelidir.
3.4.2.2	1	Verilere Yetkili Erişim	IoT sistemlerinde depolanan verilerin güvenliğinin sağlanması için yetkilendirme sağlanmalıdır.
3.4.3. Kimlik Doğrulama ve Yetkilendirme			

3.4.3.1	1	Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi	Sistemde tanımlı ise oturum sonlandırma işlemleri aktifleştirilmelidir. Bilgi güvenliğini tehdit eden bir durumun ortaya çıkması halinde oturum sonlandırma ve cihazı pasife alma işlemleri uzaktan yapılabilmelidir.
3.4.3.2	1	Kimlik Doğrulama Politikası	Güçlü kimlik doğrulama politikası tanımlanmalı ve uygulanmalıdır. Cihazın içinde iletişim için kullanılan kimlik bilgileri güvenli bir şekilde tutulmalıdır.
3.4.3.3	1	Kullanıcı Yetki Sınırlaması	Kullanıcı hesapları tekil olacak şekilde oluşturulmalı, bilgi güvenliği gereksinimleri ve cihazın yetenekleri doğrultusunda erişim yetkileri asgari düzeyde tanımlanmalıdır.
3.4.3.4	1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Ön tanımlı parolalar ve kullanıcı isimleri, kullanım öncesinde mutlaka değiştirilmeli ve kullanılan parolaların güvenli bir alanda muhafaza edilmesi sağlanmalıdır.
3.4.3.5	1	Sıfırlama Mekanizmaları	Cihaz üzerinde sıfırlama mekanizması bulunmalı ve bu mekanizmaya yetkisiz erişim engellenmelidir.
3.4.4. API ve Bağlantı Güvenliği			
3.4.4.1	1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Sistemde yerel veya bulut tabanlı web uygulamalarının varsayılan kimlik doğrulama bilgisi değiştirilmelidir.
3.4.4.2	1	API ve Bağlantı Güvenliği	API ve bağlantılarda IP kısıtlaması yapılmalıdır.
3.4.5. Diğer Güvenlik Tedbirleri			
3.4.5.1	1	Güncellemelerin Kontrolü	Sistemde varsa yeni güncelleme alma özelliği aktifleştirilmeli ve güncellemeler güvenilir kaynaklardan periyodik olarak alınmalıdır.
3.4.5.2	1	Cihazlara Fiziksel Erişimin Kısıtlanması	Cihazlara sadece yetkili kişiler fiziksel erişim sağlamalıdır. Yetkisiz kişilerin fiziksel erişimini engelleyecek güvenlik önlemleri alınmalıdır.

IoT Sunucu varlık grubu için mevcut durum ve boşluk analizi çalışması, varlık sahipleri, teknik uzmanlar ve üst düzey yöneticinin katıldığı bir çalışma grubu ile gerçekleştirilmiştir. Tablo 9.'da tedbir seviyesi 1 olan "IoT Cihazlarının Güvenliği" tedbir ana başlığındaki 16 maddenin temsili kurumun IoT yapısı dikkate alınarak değerlendirmesi yapılmıştır.

Tablo 9. IoT Sunucu varlık grubu için mevcut durum ve boşluk analizi

Tedbir No	Uygulanma Durumu T/Ç/K/H/UD)	Mevcut Duruma Yönelik Açıklama	Hedeflenen Durumu (T/Ç/K/H/UD)	Hedeflenen Durum İçin Yapılması Gereken Çalışmalar
3.4.1.1	Ç	IoT sunucunun TCP 80 ve 443 nolu portu açık. Diğer servislerin ve portların açık olup olmadığı bilinmemektedir.	T	IoT sunucu için dış hizmet alımı yöntemiyle sızma testi yaptırılacaktır.
3.4.1.2	H	Ağ servisleri için periyodik olarak açıklık kontrolleri yapılmamaktadır.	K	Ağ servislerinin zafiyet taraması için açık kaynak yazılımlar belirlenecek ve konu ile ilgili personelin eğitim alması sağlanacaktır.
3.4.1.3	K	Cihaz yapılandırmalarında uluslararası kabul görmüş en iyi uygulamalar esas alınmaktadır. Ancak IoT sunucunun kurulum, işletim ve yapılandırması için herhangi bir prosedür hazırlanmamıştır.	T	Sistem yöneticileri tarafından IoT cihazlarının kurulum ve yapılandırılması için prosedürler hazırlanacaktır.
3.4.1.4	H	IoT cihazlarının güvenli imhası veya tekrar kullanımı için herhangi bir süreç tanımlanmamıştır.	T	Kişisel Verileri Koruma Kanuna da uygun olacak şekilde verileri saklama ve imha politikası oluşturulacaktır.
3.4.1.5	K	IoT sistemleri ağa dahil edilirken sadece ilgili VLAN'ın erişmesi sağlanmaktadır. Ancak fiziksel güvenliğin olmadığı yerde yetkisiz cihazlar ağa bağlanabilmektedir.	T	IoT sistemlerinin bağlı olduğu Switch'lerde Port Security yapılandırması yapılarak port güvenliği sağlanacaktır. Ayrıca IoT cihazları erişim kontrol politikasına dahil edilecektir.
3.4.2.1	T	IoT sunucusu üzerindeki veriler düzenli olarak yedeklenmektedir.	T	Yapılması gereken herhangi bir çalışma bulunmamaktadır.

3.4.2.2	Ç	IoT sistemlerinde depolanan verilere erişim sadece yedekleme sorumlusu tarafından yapılmaktadır. Ancak erişim yetkilendirmesi herhangi bir dokümanda tanımlanmamıştır.	T	Erişim kontrol politikasına yedekleme ile ilgili yetkilendirme süreçleri eklenecektir.
3.4.3.1	T	IoT sunucusu üzerinden cihazların oturumları sonlandırılabilmektedir.	T	Yapılması gereken herhangi bir çalışma bulunmamaktadır.
3.4.3.2	K	Parola politikası dokümanında IoT cihazları için güçlü kimlik doğrulama için kurallar belirtilmemiştir. Ayrıca IoT sunucusu oturum açma ekranında kullanılan yönetici parolası kaba kuvvet saldırılarına karşı dayanıksızdır.	T	Parola politikası dokümanında IoT cihazları için güçlü kimlik doğrulama kuralları belirlenecektir. Sızma testi kapsamına IoT sunucusu da dahil edilecektir.
3.4.3.3	H	Kullanıcı hesapları tekil olacak şekilde oluşturulmamıştır. Sisteme erişim sağlayan üç sistem yöneticisi de aynı kullanıcı adı ve parola bilgisi kullanmaktadır.	T	Her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanması yapılacaktır.
3.4.3.4	H	IoT cihazlarının IoT sunucusuna kaydolabilmesi için sunucu kimlik doğrulamada varsayılan kullanıcı adı ve parola bilgisi kullanılmaktadır.	T	Tüm IoT cihazlarda varsayılan kullanıcı adı ve parola bilgileri değiştirilecektir.
3.4.3.5	UD	Cihaz üzerinde sıfırlama mekanizması bulunmamaktadır.	UD	Yapılması gereken herhangi bir çalışma bulunmamaktadır.

3.4.4.1	H	Bulut tabanlı bir API iletişimi bulunmamaktadır. IoT cihazlarında kimlik doğrulamada varsayılan kullanıcı adı ve parola bilgisi kullanılmaktadır.	T	Varsayılan kullanıcı adı ve parola bilgileri değiştirilecektir.
3.4.4.2	T	API ve bağlantılarda IP kısıtlaması yapılmaktadır.	T	Yapılması gereken herhangi bir çalışma bulunmamaktadır.
3.4.5.1	T	IoT sistem bileşenlerine ait yazılımların belirli periyotlarla güncel olup olmadığı kontrol edilmektedir. Gerekiyorsa manuel olarak güncellemeler yapılmaktadır.	T	Yapılması gereken herhangi bir çalışma bulunmamaktadır.
3.4.5.2	T	IoT cihazlarının konumlandırılması fiziksel erişim zor olacak şekilde yapılmıştır. Ayrıca kritik cihazların bulunduğu ortamlar güvenlik kameraları ile izlenmektedir.	T	Yapılması gereken herhangi bir çalışma bulunmamaktadır.

6.2.5. IoT varlık gruplarına yönelik uygulama yol haritasının oluşturulması

Tablo 9. ile ortaya konan IoT Sunucu varlık grubu için mevcut durum ve boşluk analizi çalışması, kurum üst yönetimine yeni sorumluluklar yüklemektedir. Bu çalışma sonrası kurumun Rehber uyumluluğu için yapması gereken faaliyetleri planlaması gerekmektedir. Yapılacak faaliyetler Rehber uygulama yol haritasının da kapsamını belirlemektedir. Bu çalışmada da özellikle tedbir maddeleri için yapılması gerekenler belirlenirken fayda-maliyet unsuru göz önünde bulundurulmuştur. Rehber'de belirtilen EK-C.4'teki form kullanılarak yapılması gereken iş paketleri açıkça belirtilmelidir. Bu çalışmada da Tablo 10.'daki IoT varlık gruplarına yönelik uygulama yol haritasının oluşturulmasında, Tablo 9.'daki tespitlerden yararlanılmıştır.

Tablo 10. IoT varlık gruplarına yönelik uygulama yol haritası

İş Paketi No	İş Paketi Adı	İş Paketinin Kapsadığı Faaliyetler	İş Paketi Hedefleri	
1	IoT Sunucu Güvenliği	Sıkılaştırma	2.Ay	Tüm IoT cihazlarında varsayılan kullanıcı adı ve parola bilgileri değiştirilecektir.
			3.Ay	IoT sistemlerinde her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanması yapılacaktır.
			6.Ay	Switch'lerde Port Security yapılandırması için çalışma yapılacaktır.
		Dokümantasyon	7.Ay	Parola politikası dokümanında IoT cihazları için güçlü kimlik doğrulama kuralları belirlenecektir.
			8.Ay	Erişim kontrol politikası, IoT sistemleri ile ilgili kimlik yetkilendirme süreçleri kapsamında güncellenecektir.
			9.Ay	IoT cihazlarının kurulum ve yapılandırılması için prosedürler hazırlanacaktır.
			10.Ay	Verileri saklama ve imha politika dokümanı oluşturulacaktır.
		Hizmet Alımı	12.Ay	Dışarıdan sızma testi hizmet alımı yapılacaktır.
		Ürün Tedariki	15.Ay	Zafiyet yönetimi için açık kaynak yazılımlar belirlenip kullanılacaktır.
		Eğitim	18.Ay	Üç teknik personelin "Uygulamalı Sızma Testi Eğitimi" alması sağlanacaktır.

7. SONUÇ VE ÖNERİLER

Ulusal Bilgi ve İletişim Güvenliği Rehberi; oldukça fazla teknik tedbirin yer aldığı, hemen hemen bilgi teknolojilerindeki her alana dokunduğu, güvenlik tedbirlerinin ürün ve teknolojiden bağımsız seçimine olanak verdiği, ortak mutabakat ile hazırlanması ve ulusal/uluslararası mevzuat ve standartlara uyumlu olması gibi özellikleri nedeniyle güçlü bir rehber niteliğindedir. Bu çalışmada da Rehber'in yapısı ve uygulama süreçlerinden bahsedilerek örnek bir senaryo üzerinden Rehber uyum çalışmasının nasıl yapılacağına dair gösterim yapılmıştır.

Ayrıca Rehber'in geliştirilmesine ve sürdürülebilirliğine katkıda bulunmak için aşağıdaki tespit ve önerilere yer verilmiştir:

- TEMPEST gibi bazı güvenlik maddelerinin tedbir seviyesinin 1. veya 2. derecede olması kamu kurum ve kuruluşlarının fayda maliyet açısından uygulamasını zorlaştırmaktadır. Dolayısıyla Rehber'deki tedbir seviyelerinin tekrar gözden geçirilip uygulayıcılarının çoğunun kamu kurumu olduğu da düşünülerek yeniden değerlendirilmesi gerekmektedir.

- Rehber'deki tedbir maddeleri sadece insan ve teknoloji odaklı varlıklar dikkate alınarak belirlendiği için bilgi güvenliği yönetişimine Rehber'de pek yer verilmemiştir. "Siber Olay Yönetimi", "İş Sürekliliği Yönetimi", "Kişisel Veri Yönetim Sürecinin İşletilmesi" gibi yönetsel konular Rehber'de yer alsa da risk yönetimi, süreç yönetimi, bütçe yönetimi gibi bilgi teknoloji süreçlerinde önemli etkiye sahip yönetişim konuları bulunmadığı için kurumların bilgi güvenliğini sağlamada bütüncül bir yaklaşım ortaya koyması zor olacaktır.

- Rehber'de "Kritik Altyapılar Güvenliği" ve "Yeni Geliştirmeler ve Tedarik" ana başlıklarındaki güvenlik tedbirleri, Rehber'deki diğer ana başlıklara bakıldığında oldukça yetersiz görülmektedir. Özellikle kritik altyapıları ilgilendiren tedbir maddelerinin sektöre özel maddelerden oluşması gerekmektedir.

- Rehber'de yer alan işletim sistemleri, veri tabanları, web sunucuları ve sanallaştırma sistemlerine yönelik sıkılaştırma tedbirlerinin uygulanabilmesi için kurumların sıkılaştırma kılavuzlarını hazırlamaları gerekmektedir. Bu konuda CIS Benchmark dokümanlarından yararlanılabilse bile İngilizce ve çok detaylı olması nedeniyle bu dokümanlar, pratikte kurumlar tarafından doğrudan kullanılamamaktadır. Hali hazırda Türkçe sıkılaştırma kılavuzlarının olmaması, sıkılaştırma dokümanlarının hazırlanmasının oldukça zaman alması ve ayrı bir uzmanlık alanı olması nedeniyle genel olarak her kurumun kullanabileceği nitelikte sıkılaştırma kılavuzlarının Dijital Dönüşüm Ofisi tarafından hazırlanıp kullanıma açık hale getirilmesi, Rehber'in uygulanabilirliğine katkı sağlayacaktır.

- Bilgi ve İletişim Güvenliği Denetim Rehberi'nde denetim faaliyetlerinin iç denetim yoluyla yapılması vurgulanmaktadır. Ancak kurumların belirli periyotlarla bağımsız dış denetime tabii tutulması gerekliliği ile ilgili herhangi bir açıklamada bulunulmamaktadır. Şeffaf, açık ve bağımsız dış denetim sürecinin belirlenmesi, kurumların denetim faaliyetlerine değer katacaktır.

- Kurumların Rehber'de belirtilen süreçleri yerine getiremediğinde veya tedbir maddeleri ile ilgili uygunsuzluk durumunda nasıl bir müeyyide ile karşılaşacağı açık bir şekilde ifade edilmemiştir. Ayrıca Dijital Dönüşüm Ofisi'nin sorumluluğunda olan Rehber uyumluluğu kapsamında gözetim faaliyetini nasıl gerçekleştireceği de tam olarak belli değildir. Bu durum yerleşik kamu kültüründe atalete sebep olabileceği gibi Rehber'e uyum süreçlerini de yavaşlatacaktır. Yasal mevzuatın bu konudaki sorunlara çözüm olacak şekilde uygun hale getirilmesi gerekmektedir.

- Rehber'in hedeflerinden biri olan yerli ve milli siber güvenlik ürünlerinin kamuda kullanımının yaygınlaştırılması çalışmasını desteklemek için Bilgi ve İletişim Güvenliği Rehberi'nde, kullanılabilecek Türkiye Siber Güvenlik Kümelenmesinde yer alan yerli ürünler kataloğunun oluşturulması gerekmektedir. Ayrıca tedbir maddelerinin denetim faaliyetlerinde kullanılabilecek açık kaynak yazılımların da Rehber'de belirtilmesi, sınırlı bütçeye sahip kamu kurum ve kuruluşları için büyük bir kolaylık olacaktır.

- Aralık 2022 sonuna kadar Rehber denetiminin kurumlarca tamamlanmasının akabinde, Dijital Dönüşüm Ofisi tarafından hem Rehber uygulama sürecinde yaşanan sorunların ele alındığı hem de gelecekte ortaya çıkabilecek problemlere çözüm önerilerinin tartışıldığı kurumlar arası tecrübe paylaşım ortamının oluşturulması, Rehber uyumunda standartlaşmayı sağlayacaktır.

- Yeni oluşturulacak Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda siber uzay güvenliği için kurumların Rehber uyum çalışmalarına ve denetim faaliyetlerine yer verilmelidir.

Bu çalışmayla ilk kez Bilgi ve İletişim Güvenliği Rehberi bir makalede detaylı olarak ele alınmıştır. Ayrıca Rehber'deki IoT güvenliğine yönelik tedbir maddeleri, simülasyon ortamı oluşturularak Rehber uygulamasının nasıl olacağı temsili bir kamu kurumu üzerinde gösterilmiştir. Özellikle Rehber'deki tedbir maddelerinin çokluğu ve tüm tedbir maddelerinin tek bir çalışmada ele almanın zorluğu nedeniyle bundan sonra yapılacak çalışmalarda Rehber'de yer alan diğer ana başlıklardaki güvenlik tedbirleri konu edilebilir. Bunun yanı sıra Rehber'in uygulanması ve denetimi ile ilgili kamu kurumları ile kritik altyapı niteliğinde hizmet veren işletmelere yönelik anket çalışması yapılarak kurumların Rehber'e bakışları ve Rehber uyumuna yönelik eğilimleri ela alınabilir.

Bu çalışmayla Ulusal Bilgi ve İletişim Güvenliği Rehberi'nin daha fazla bilinip anlaşılmasına katkıda bulunmanın yanı sıra Rehber içeriğinin geliştirilmesine yönelik çalışmaların sayısını arttırmaya öncülük etmesi temenni edilmektedir.

Yazarların Katkısı

Yazarların makaleye olan katkıları eşit orandadır.
Bu çalışmada Prof. Dr. Abdül Halim ZAİM, Doç. Dr. Muhammed Ali AYDIN fikir, eleştiri ve makalenin yazımı konusunda katkıda bulunmuştur. Muttalip TULGAR araştırma, analiz, yorum, kaynak taraması ve makalenin yazımı konusunda katkı sağlamıştır.

Teşekkür

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'ne çalışmaya verdikleri destek için teşekkürü bir borç bilmekteyiz.

Çıkar Çatışması Beyanı

Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır.

Araştırma ve Yayın Etiği Beyanı

Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

KAYNAKÇA

Ağdeniz, Ş. (2021). Bilgi ve iletişim güvenliği denetiminde kamu iç denetçilerinin rolü ve yetkinliklerine ilişkin bir araştırma. *Alanya Akademik Bakış,* 5(2), 525-545.

Avcı, İ. (2022). Akıllı evlerde IoT teknolojileri ve siber güvenlik. *Avrupa Bilim ve Teknoloji Dergisi,* 34, 226-233.

Asma Haroon, Munam Ali Shah, Yousra Asim, Wajeeha Naeem, Muhammad Kamran & Qaisar Javaid. (2016). Constraints in the IoT: The world in 2020 and beyond. *International Journal of Advanced Computer Science and Applications* (IJACSA, 7(11). http://dx.doi.org/10.14569/IJACSA.2016.071133

CIS (Center for Internet Security) (2021). CIS Controls. https://www.cisecurity.org/controls/cis-controls-list adresinden 11 Mayıs 2022 tarihinde alınmıştır.

Cisco (2022). Cisco packet tracer frequently asked questions. https://www.netacad.com/sites/default/files/cisco-packet-tracer-faq.pdf adresinden 21 Haziran 2022 tarihinde alınmıştır.

CMMC (Cybersecurity Maturity Model Certification) (2021). CMMC model overview. https://www.acq.osd.mil/cmmc/docs/ModelOverview_V2.0_FINAL2_20211202_508.pdf adresinden 05 Mayıs 2022 tarihinde alınmıştır.

CSA (Cloud Security Alliance), (2021). Cloud controls matrix. https://cloudsecurityalliance.org/download/artifacts/cloud-controls-matrix-v4/ adresinden 11 Mayıs 2022 tarihinde alınmıştır.

DDO (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi) (2020). Bilgi ve iletişim güvenliği rehberi. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf adresinden 02 Nisan 2022 tarihinde alınmıştır.

DDO (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi) (2021). Bilgi ve iletişim güvenliği denetim rehberi. https://cbddo.gov.tr/SharedFolderServer/Projeler/File/BG_Denetim_Rehberi.pdf adresinden 10 Nisan 2022 tarihinde alınmıştır.

DDO (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi) (2021). TS EN ISO/IEC 27001:2017 Kontrolleri ile Bilgi ve İletişim Güvenliği Rehberi Eşleştirme Tablosu. https://cbddo.gov.tr/SharedFolderServer/Projeler/File/ISO27001%20-%20BGRehberEslestirmeTablosu.pdf adresinden 17 Nisan 2022 tarihinde alınmıştır.

ENISA (2017). Security aspects of virtualization. https://www.enisa.europa.eu/publications/security-aspects-of-virtualization/@@download/fullReport adresinden 01 Mayıs 2022 tarihinde alınmıştır.

ISO/IEC 27001, 2017. Information technology -Security techniques - Information security management systems - Requirements

Kaymas, S. (2020). Kamu yönetişiminin uzamı ve aracı olarak nesnelerin interneti politikaları üzerine bir değerlendirme. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi,* 7 (1) , 74-94 . DOI: 10.17336/igusbd.675949

NIST SP 800-125 (2011). Guide to security for full virtualization technologies. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf adresinden 12 Mayıs 2022 tarihinde alınmıştır.

NIST SP 800-82 (2015). Guide to ındustrial control systems (ICS) security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf adresinden 12 Mayıs 2022 tarihinde alınmıştır.

NIST SP 800-53 (2020). Security and Privacy controls for ınformation systems and organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf adresinden 12 Mayıs 2022 tarihinde alınmıştır.

OWASP (2021). OWASP application security verification standard. https://github.com/OWASP/ASVS/raw/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf adresinden 01 Mayıs 2022 tarihinde alınmıştır.

OWASP (2021). OWASP ınternet of things security verification standard. https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS adresinden 01 Mayıs 2022 tarihinde alınmıştır.

OWASP (2022). OWASP mobile app security checklists. https://github.com/OWASP/owasp-mstg/releases/tag/v1.4.0 adresinden 01 Mayıs 2022 tarihinde alınmıştır.

Özdoğan, E. & Daş, R. (2021). IoT based a smart home automation system design: Simulation case. *Balkan Journal of Electrical and Computer Engineering,* 9(3), 297-303. DOI: 10.17694/bajece.918826

STIG (2022). STIGs document library. https://public.cyber.mil/stigs/downloads/ adresinden 01 Mayıs 2022 tarihinde alınmıştır.

Thera, D. (2020). *Internet of things simulation using Cisco packet tracer* [Yüksek lisans tezi]. İzmir Yüksek Teknoloji Enstitüsü. İzmir.

Ülker, M., Canbay, Y. & Sağıroğlu, Ş. (2017). Nesnelerin internetinin kişisel, kurumsal ve ulusal bilgi güvenliği açısından incelenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 10 (2) , 28-41.

Wikipedia (2022). OWASP. https://en.wikipedia.org/wiki/OWASP adresinden 01 Mayıs 2022 tarihinde alınmıştır.

Zeybek, M. & Yılmaz, E. N. (2019). Nesnelerin interneti: Risk temelli yaklaşım. *Denetişim,* 0 (19), 73-88.