Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi

(DÜSBED) ISSN : 1308-6219

Nisan 2015
YIL-7 S.13

SOSYAL GÜVENLİK KURUMUNDAKİ SİBER GÜVENLİK YÖNETİMİ UYGULAMALARININ İNCELENMESİ VE DEĞERLENDİRİLMESİ

Halil İbrahim MİL[1]

Öz

Siber uzay gün geçtikçe hayatımızın içerisine daha fazla girmektedir. İnsanlar artık alışverişlerini, haberleşmelerini ve daha birçok resmi ve özel işlemlerini internet üzerinden gerçekleştirmektedir. Bu nedenle günümüzde birçok kamu kurumu iş ve işlemlerini bilişim sistemleri üzerinden sunmaktadır. Bu kurumlardan bir tanesi de Türkiye nüfusunun tamamına yakınına hizmet veren Sosyal Güvenlik Kurumu'dur. Sosyal Güvenlik Kurumu, vatandaşların kişisel bilgileri, sosyal sigorta ve sağlık sigortası bilgileri gibi birçok veriyi barındırmaktadır, dolayısıyla özellikle Sosyal Güvenlik Kurumu'nda siber güvenlik yönetimi ve uygulamaları çok önemlidir.

Bu çalışmanın amacı; Sosyal Güvenlik Kurumu'ndaki siber güvenlik uygulamalarını ortaya koymak ve konuyla ilgili değerlendirme ve öneriler yapmaktır.

Anahtar Kelimeler: Sosyal Güvenlik Kurumu, Siber Güvenlik

EXAMINING AND EVALUATING OF PRACTICES CYBER SECURITY MANAGEMENT IN SOCIAL SECURITY INSTITUTION

Abstract

Cyber space enters more into our lives day by day. People performs their shoppings, communications and many other public and private transactions over the internet. Therefore, nowadays many public institutions offers business and transactions over the information systems. Social Security Institution is one of these organizations, which serves almost all of Turkey's population. Social Security Institution contains many data like the personal information, social insurance and health insurance informations of citizens, thus especially cyber security management and practices in the Social Security Institution is very important.

The aim of this study is to reveal the cyber security practices in Social Security Institution and evaluate and advise on the subject.

Key Words: Social Security Institution, Cyber Security

GİRİŞ

Bilgi çağı olarak da adlandırılan günümüz dünyasında, teknoloji hemen her alanda karşımıza çıkmaktadır. İnsanlar, kamu kurumları ile olan işlerinin çoğunu bilgisayarlar, tabletler ve akıllı telefonlar üzerinden halletmektedir. İnsanların ihtiyaçlarının gün geçtikçe artması, teknolojinin gelişmesi, internetin ortaya çıkması, sosyal ağların gelişmesi, insanların anlık olarak birbirlerinden haber alabilmesi, devlet kurumlarının da sunmuş olduğu hizmetleri siber uzayda

[1] Dr., Müfettiş, Sosyal Güvenlik Kurumu, Simon Bolivar Cad. No:23 Çankaya/Ankara, hibrahimmil@gmail.com

sunmasını zorunlu kılmıştır. Bu sebeplerle günümüzde banka işlemleri, gsm işlemleri, sosyal güvenlik, emniyet, adalet, eğitim ile ilgili işlemler vb. birçok işlemler günümüzde siber uzayda sunulmaya başlanmıştır.

Bütçesi ve hizmet verdiği insan sayısı açısından devletin önemli kurumlarından biri olan Sosyal Güvenlik Kurumu da vatandaş odaklı çalışma anlayışının gereği olarak birçok hizmetini siber uzayda sunmaktadır. SGK her geçen gün bu hizmetlerini arttırarak sunmaya devam etmektedir. Peki, bu kadar geniş kapsamlı hizmetlerin elektronik ortamda sunulması ne derece güvenlidir? Bu hizmetlere erişim durdurulduğunda ne gibi sorunlarla karşı karşıya kalınabilir? Sosyal Güvenlik Kurumu'nun siber güvenlik uygulamaları ve politikaları nelerdir? gibi soruların cevapları hakkında düşünmek ve gerekli tedbirleri almakta fayda vardır.

Bu çalışmada Sosyal Güvenlik Kurumu'nun siber güvenlik bağlamında yönetimi, uygulama ve politikaları incelenecek ve değerlendirilecektir. İlk bölümde siber güvenliğin kavramsal çerçevesi çizilecek, ikinci bölümde Sosyal Güvenlik Kurumundaki siber güvenlik yönetimi yapılanması anlatılacak ve son bölümde ise kurumdaki siber güvenlik uygulamaları ve politikalarına değinilecektir. Çalışmada araştırma yöntemlerinden ikincil veri analizi ve içerik analizi kullanılacaktır. Siber güvenlik alanında ve kurumsal siber güvenlik analizi konusunda akademik olarak pek fazla çalışmanın olmaması makaleyi ayrıca anlamlandırdığı düşünülmektedir.

1. SİBER GÜVENLİK İLE İLGİLİ KAVRAMLAR

1.1. Siber Güvenlik

Siber güvenlik kavramı, her türlü kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve devam ettirilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri arasında erişilebilirlik, bütünlük ve gizlilik yer almaktadır (Bilgi Teknolojileri ve İletişim Kurumu, 2014). Erişilebilirlik hedefi, saklanan bilginin sadece yetkili kişilerce ulaşılabilir olması gerekliliğini ifade etmektedir. Bütünlük hedefi, bilişim sistemleri vasıtasıyla depolanan bilginin değiştirilmemiş, kısmen veya tamamen de olsa silinmemiş, yok edilmemiş olmasıdır. Gizlilik hedefi ise bilgiye sadece ilgili kişilerce erişilebilmesi anlamındadır (Hekim ve Başıbüyük, 2013:137). Siber güvenlik, siber uzaydan gelebilecek tehditlere karşı insanları, kurum ve kuruluşları korumak maksadıyla oluşturulan strateji ve politikalardan meydana gelmektedir (Bakır, 2012:13).

Diğer taraftan, siber güvenlik kavramı bireyler, kurumlar ve devletler açısından farklı olarak yorumlanabilir. Siber güvenlik bireyler açısından kendilerini güvenli hissetmek, kişisel verileri korumak; kurumlar açısından işle ilgili önemli işlevlerin kullanılabilir olmasını, operasyon ve bilgi güvenliği sayesinde gizli verilerin korunmasını sağlamak; devletler açısından ise tüm bilgisayar sistemlerinin ve kritik altyapıların saldırılara ya da verilerin çalınmasına karşı korunması anlamındadır (Storch, 2012:3).

Siber güvenlik kavramı Türkiye'de ve dünyada önemini hissettirmeye başlayan bir olgudur. Türkiye'de siber güvenlik alanının bütünüyle ele alacak kadar kapsamlı bir mevzuat altyapısı bulunmamaktadır ve bununla birlikte adli ve

kolluk personellerinin de yeteri kadar bilgi ve uzmanlığa sahip olmadığı gözlenmektedir (Ünver, Canbay ve Mirzaoğlu, 2009:42).

1.2. Siber Uzay

Uluslararası alanda kabul edilmiş bir siber uzay tanımı bulunmamaktadır. Farklı uluslararası otoriteler tarafından yapılmış çeşitli tanımlar mevcuttur. Ayrıca, 'Siber Uzay' kavramı yerine 'Siber Alan' veya 'Siber Ortam' ifadeleri de kullanılmaktadır.

Siber uzay kavramı 2003 yılında Beyaz Saray tarafından "kritik altyapılarımızın çalışmasını sağlayan, birbirine bağlı yüz binlerce bilgisayar, sunucu, yönlendirici (rooter), anahtar (switch) ve fiber optik kablolardan oluşur" şeklinde tanımlanmıştır (The White House, 2003:vii). 2006 yılında ABD Savunma Bakanlığı tarafından, "İletişim ağı ile birbirine bağlanan sistemlerde, veri saklama, değiştirme ve iletme amacıyla elektronik ve elektromanyetik spektrumun kullanıldığı alandır" şeklinde tanımlanmıştır (US DoD, 2006:ix). 2010 yılında ABD Savunma Bakanlığı tarafından, "İnternet, iletişim ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağlı ağların oluşturduğu bilgi ortamındaki küresel bir alandır" şeklinde tanımlanmıştır (US DoD, 2010:63).

1.3. Siber İstihbarat

Erişim izni olmaksızın kişisel, ekonomik, politik veya askeri saiklerle bilgisayarlara veya iletişim ağlarına illegal olarak sızmak suretiyle, şahısların, grupların ve ülkelerin sırlarını elde etme eylemi siber istihbarat olarak ifade edilmektedir (Çifci, 2013:6). Teknolojinin gelişmesiyle ülkelerin siber istihbarat çalışmaları üzerinde önemle durdukları bilinmektedir. Dünyadaki tüm bilgisayarların birbirine bağlı olması, daha az maliyetli olması ve siber uzayın kullanıcılara anonimlik sağlaması gibi faktörler siber istihbarat kavramının önemini arttırmaktadır.

1.4. Siber Terör

Terör faaliyetlerinin siber uzay kullanılarak gerçekleştirilmesi siber terörizm olarak adlandırılmaktadır. Burada siber terör kavramı terör örgütlerinin siber alanı araç olarak kullanmaları söz konusudur (Kaya, 2012:22).

1.5. Siber Savaş

Geleceğin savaşları artık bilişim sistemleri üzerinden yapılacağı tahmin edilmektedir. Çünkü, devletler, kurumlar, şirketler ve bireyler iş ve işlemlerini bu sistemler üzerinden yapmakta; bağımlı halde hayatlarını sürdürmektedir (Ege, 2012:18). 21. yüzyılın başları siber savaş olgusunun ortaya çıktığı ve geleceğe yönelik derin etkilerin meydana geldiği sıra dışı bir zaman dilimi olarak tarihte yerini alacaktır (Bilgi Güvenliği Derneği, 2012:4). Siber savaş, siber uzayı ve içindeki varlıkları korumak için yapılan çalışmaların geneli için kullanılan bir ifadedir. Bu çalışmaların geneli siber savaş olarak adlandırılmakla birlikte siber savaşta hedeflenen, ülkelerin güvenlik, sağlık, enerji, ulaşım, haberleşme, su, bankacılık, kamu hizmetleri gibi kritik sektörlerinin bilgi sistem altyapılarıdır (Bakır, 2014). Siber savaş, bir devletin başka bir devletin bilgisayar sistemlerine

veya ağlara hasar vermek ya da kesinti oluşturmak üzere gerçekleştirilen sızma faaliyetleri olarak tanımlanabilir (Clarke ve Knake, 2010:11).

1.6. Kritik Altyapılar

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında, "İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" kritik altyapı olarak tanımlanmıştır.

Kritik altyapılar ülkeden ülkeye değişmekle beraber, bunlar genellikle kamu kurumları, bankacılık, adalet, güvenlik, enerji, finans, su, gıda sektörleri olduğu kabul edilmektedir. Bu sektörlerin tamamı bilgi işlem altyapıları ile çalışmakta olduğundan ülkelerin en kritik altyapılar olarak değerlendirilmektedir.

Son yıllarda kullanılmaya başlanan UYAP, MERNİS, ASAL ve MEDULA gibi vatandaşlara ait birçok bilgiyi içeren bilgi işlem altyapılarının geliştirilmesi Türkiye'de de kritik altyapılara sahip sektörlerin bulunduğunu göstermektedir (Ünver ve Canbay, 2010:96).

2. SOSYAL GÜVENLİK KURUMU (SGK) VE SİBER GÜVENLİK YÖNETİMİ

Sosyal Güvenlik Kurumu, ülke nüfusunun büyük bir kısmını kapsamı altına almaktadır. Bu nedenle, yürütülen sosyal güvenlik hizmetlerine ilişkin işlem hacmi ve evrak yoğunluğunun çok büyük bir boyutta olması kaçınılmazdır. Bu çerçevede, SGK tarafından bilgi teknolojilerinin etkin bir biçimde kullanılması bir zorunluluktur. Bu kapsamda, Kuruma bağlı merkez ve taşra ünitelerine, sağlık hizmet sunucularına, işverenlere ve sosyal güvenlik kapsamında bulunan vatandaşlara yönelik yazılım projelerinin hayata geçirilerek kullanıma sunulması ve güvenliğinin sağlanması görevi kurumun ana hizmet birimlerinden Hizmet Sunumu Genel Müdürlüğü tarafından yerine getirilmektedir.

5502 sayılı Sosyal Güvenlik Kurumu Kanununa göre Kurum Başkanına yardımcı olmak üzere üç başkan yardımcısı görevlendirilmektedir. Başkan yardımcılarının her biri kurumun farklı Genel Müdürlüklerinden ve Daire Başkanlıklarından sorumlu olarak çalışmalarını sürdürmektedir. Bu doğrultuda, Sosyal Güvenlik Kurumunun siber güvenlik yönetimi Kurum Başkanının takibi ve ilgili Başkan Yardımcısının sorumluluğunda, Hizmet Sunumu Genel Müdürlüğü çatısı altında yürütülmektedir. Hizmet Sunumu Genel Müdürlüğü de bünyesinde barındırdığı Daire Başkanlıkları vasıtasıyla siber güvenlik çalışmalarını sürdürmektedir.

2.1. Kurumun Yönetim ve Organizasyon Yapısı

Sosyal Güvenlik Kurumu'nun Çalışma ve Sosyal Güvenlik Bakanlığı'nın ilgili kuruluşu olduğu 5502 sayılı Sosyal Güvenlik Kurumu Kanunu'nda belirtilmiştir. Sosyal Güvenlik Kurumu, her ne kadar Çalışma ve Sosyal Güvenlik Bakanlığı'nın çatısı altında yer alsa da kamu tüzel kişiliğini haiz, idarî ve malî açıdan özerk, bu

Kanunda hüküm bulunmayan durumlarda özel hukuk hükümlerine tabi olarak iş ve işlemlerini yürütmektedir.

SGK'nın organları 5502 sayılı Kanunun 4. maddesinde, Genel Kurul, Yönetim Kurulu ve Başkanlık olarak sıralanmıştır. Başkanlık teşkilatı, merkez ve taşra teşkilatından meydana gelmektedir. Başkanlık merkez teşkilâtı ise ana hizmet birimleri ile danışma ve yardımcı hizmet birimlerinden meydana gelir.

Kurumun Merkez Teşkilatında yer alan ana hizmet birimleri şunlardır (SGK, 2013a:6):

a) Emeklilik Hizmetleri Genel Müdürlüğü

b) Sigorta Primleri Genel Müdürlüğü

c) Genel Sağlık Sigortası Genel Müdürlüğü

ç) Hizmet Sunumu Genel Müdürlüğü

d) Rehberlik ve Teftiş Başkanlığı

e) Aktüerya ve Fon Yönetimi Daire Başkanlığı

5502 sayılı Kanunun 27. maddesine göre Başkanlık Taşra Teşkilatı her ilde kurulan Sosyal Güvenlik İl Müdürlükleri ile Sosyal Güvenlik İl Müdürlüklerine bağlı olarak kurulacak olan Sosyal Güvenlik Merkezlerinden oluşmaktadır. Sosyal Güvenlik Merkez Müdürlükleri, il ve ilçelerde nüfus, sigortalı ve genel sağlık sigortalısı sayısı, işyeri sayısı, işlem yoğunluğu ve belirlenecek diğer kriterler doğrultusunda kurulur veya kaldırılır.

2.2. Hizmet Sunumu Genel Müdürlüğü (HSGM)

Hizmet Sunumu Genel Müdürlüğü'nün amacı, gerçek ve tüzel kişilere yönelik hizmet sunumunun kesintisiz olarak yerine getirilmesi, verilen hizmetlerin kaliteli ve kolay erişilebilir olmasını sağlamaktır. HSGM bu amaçtan hareketle, bilgi teknolojilerini etkin bir şekilde kullanmaktadır. Teknolojinin etkin kullanımıyla, kurum hizmetlerinin iş süreçlerine bağlı elektronik ortamda, kullanıcı ihtiyaçları göz önünde bulundurularak çevrimiçi, kesintisiz, güvenli ve çoklu ortamlardan erişilebilir nitelikte ve tek bir nokta üzerinden vatandaşlara ulaştırılması sağlanmaktadır. Tüm sigorta prim bildirimleri ve tahsilatların takip edildiği e-bildirge ve işveren sistemi; tüm sağlık ödemelerinin belirlenen kurallar çerçevesinde yürütülmesine yönelik olarak da MEDULA uygulaması (medula-hastane, medula-eczane, medula-optik) gibi uygulamaları kesintisiz olarak sunmaktadır. Ayrıca, bu uygulamaların yenilenmesi ve güçlendirilmesi çalışmalarına devam edilmektedir (SGK, 2015a).

2.2.1. Görev, Yetki ve Sorumluluklar

SGK'nın siber güvenlik yönetiminden sorumlu organı olan Hizmet Sunumu Genel Müdürlüğü'nün görevleri 5502 sayılı kanunun 16. maddesinde aşağıdaki şekilde sıralanmıştır.

a) Kurumun gerçek ve tüzel kişilere yönelik hizmet sunumunun kesintisiz olarak yerine getirilmesini sağlamak.

b) Hizmet sunumuna ilişkin konularda, performansın geliştirilmesine yönelik olarak ilgili birimler ile birlikte iş süreçlerini belirlemek, yürütülen işlerle ilgili verileri toplamak, analiz etmek, elde ettiği sonuçları ilgili birimlerle paylaşarak iş süreçlerini geliştirmek.

c) Taşra teşkilâtı birimlerinin kurulması ve kapatılması ile ilgili iş ve işlemleri yürütmek.

ç) Kurum merkez ve taşra teşkilâtının her türlü bilişim hizmetlerini yürütmek.

d) Sosyal güvenlik veri tabanını oluşturmak, diğer kamu idarelerinin veri tabanları ile entegrasyonunu sağlamak, sosyal güvenlik veri tabanı bilgilerinin güncelliğini sağlamak ve Kurum faaliyetlerinin etkililiğini artıracak şekilde kullanıma sunmak.

e) Kurum için gerekli yazılım ve donanım altyapılarını plânlamak, geliştirmek, kurmak, işletmek, yenilemek, bu altyapıların güvenliğini ve sürekliliğini sağlamak üzere gerekli önlemleri almak.

f) Görev konusuyla ilgili uygulamaları izlemek ve geliştirmek.

g) Başkan tarafından verilecek benzer nitelikteki diğer görevleri yapmak.

2.2.2. Teşkilat Yapılanması

Hizmet Sunumu Genel Müdürlüğü'nün idari yapısı Genel Müdür, 2 Genel Müdür Yardımcısı ve 11 adet Daire Başkanlığından oluşmaktadır. Genel Müdürlük bünyesinde yer alan daire başkanlıkları şunlardır: Bilgi Sistemleri ve Siber Güvenlik Daire Başkanlığı, Bilgilendirme ve Koordinasyon Daire Başkanlığı, Emeklilik Yazılımları Daire Başkanlığı, Veri Yönetimi Daire Başkanlığı, İş Geliştirme Daire Başkanlığı, Sağlık Yazılımları Daire Başkanlığı, Kurumsal Yazılımlar Daire Başkanlığı, Muhasebe Yazılımları Daire Başkanlığı, Sigorta Yazılımları Daire Başkanlığı, Risk Yönetimi ve Proje Daire Başkanlığı, Yönetim Hizmetleri Daire Başkanlığı (SGK, 2015b).

Hizmet Sunumu Genel Müdürlüğü bünyesinde 555 Memur, 117 Sözleşmeli Personel ve 1 adet işçi olmak üzere toplam 673 kişi görev yapmaktadır (SGK, 2014a:6). Diğer taraftan, 2014 yılı performans programında Bilişim Teknolojileri Faaliyetleri için toplam kaynak ihtiyacı 36.525.800-TL olarak belirlenmiştir. Bu tutar 2014 yılı bütçe ödeneğinin %0,02'sine tekabül etmektedir (SGK, 2014a:49).

2.2.3. Bilgi Sistemleri ve Siber Güvenlik Daire Başkanlığı

Siber güvenlik ile ilgili çalışmaların merkezinde Hizmet Sunumu Genel Müdürlüğü bünyesinde yer alan Bilgi Sistemleri ve Siber Güvenlik Daire Başkanlığı yer almaktadır. Bu daire başkanlığı bünyesinde siber güvenlik ve kalite şube müdürlüğü oluşturulmuştur. Bununla birlikte, konunun önemi ve tüm birimleri ilgilendirmesi dolayısıyla diğer daire başkanlıklarında da siber güvenlik ve kalite ekibi adı altında yeni birimler oluşturulmuştur. Bilgi Sistemleri ve Siber Güvenlik Daire Başkanlığı'nın görevleri aşağıda sıralanmıştır (SGK, 2014b:77):

a) Kurumun donanım ve sistem altyapısına yönelik ihtiyaç analizlerini yaparak, projelendirme talebini ilgili birime bildirmek ve takibini yapmak.

b) Fiziksel altyapı ve sistemin güvenlik politikalarını belirlemek ve uygulamak. Bilgi güvenliği yönetim sistemi çerçevesinde, yürütülen iş ve işlemlere ilişkin bilgi güvenliği tedbirlerini diğer daire başkanlıkları ile koordineli olarak almak.

c) Daire başkanlığı görev alanına giren bilişim hizmetlerinin kesintisiz olarak sürdürülebilmesi için gerekli tedbirleri almak.

d) Sistem ve sunucular üzerindeki yük ve kapasite analizlerini yaparak performanslarını izlemek ve gerekli düzeltici faaliyetleri yürütmek.

e) Diğer kurumlarla olan iletişim altyapısını güvenli şekilde tesis etmek.

f) Kurumsal sistemlerin ve sunucuların üzerindeki ağ, veri tabanı, sistem yazılımları, uygulama yazılımları ile diğer yedekleme işlemlerini yürütmek.

g) Bilgi sistemlerinin risk kütüklerini oluşturmak ve gerekli tedbirlerin alınmasını sağlamak.

h) Felaket durumunda Kurumun kesintisiz hizmet vermesini sağlayacak tedbirlerin alınmasını sağlamak.

j) Sunucu ve donanımların bakım, onarım iş ve işlemlerinin yürütülmesini sağlamak.

k) Daire başkanlığının görevleri kapsamında olup, stratejik plan, eylem planı, hizmet envanteri, soru önergesi ve faaliyet raporları çerçevesinde istenilen bilgiler ile denetim ve il müdürlükleri koordinasyon raporlarına ilişkin iş ve işlemleri yapmak ve talep eden birime bildirmek.

l) Kurum portalının bakımını yapmak, sistem, sunucu, veri tabanı ve güvenliğe ilişkin iş ve işlemlerini yürütmek.

m) Her türlü siber saldırılara karşı, ilgili kurum ve kuruluşlar ile işbirliği içinde çalışmak.

n) Genel Müdür/Genel Müdür Yardımcısı tarafından verilecek benzer nitelikteki diğer görevleri yapmak.

Diğer taraftan Hizmet Sunumu Genel Müdürlüğü çatısı altında faaliyet gösteren diğer daire başkanlıklarının, yürütülen iş ve işlemlere ilişkin bilgi güvenliği tedbirlerini Bilgi Sistemleri ve Siber Güvenlik Daire Başkanlığı ile koordineli olarak almaları gerekmektedir.

2.2.4. Temel Politika ve Öncelikler

SGK, teknoloji ve iş geliştirme alanında Sosyal Güvenlik Entegrasyon Projesi (SGEP) sürdürülmektedir. Projenin tamamlanarak faaliyete geçirilmesiyle birlikte, iç kontrol, iç denetim, risk denetimi, kayıt dışı ekonomiyle mücadele gibi birçok alanda daha etkin çalışmalar yapılabilecektir. Projeyle birlikte, e-Tescil, e-Prim, e-Hizmet, e-Emeklilik olmak üzere bütünleşik olarak kurgulanmış önemli bir e-Devlet paylaşım platformu kurulacaktır. Kurumun, siber güvenliğin sağlanması

hususunda önem arz eden temel ve öncelikli politikalarından bazıları şunlardır (SGK, 2014a:37):

a) Batıkent Veri Merkezi Projesinin tamamlanması,

b) "Bulut Bilişim" kapsamında Bakanlık ve diğer Kamu Kurum ve Kuruluşlarına Housting (Ev Sahipliği vb.) hizmet üreten yapıyı kurmak ve bu yapıda işletmecilik faaliyetlerini sürdürmek,

c) Siber güvenlik ve kurumsal bilgi güvenliğinin ilgili iç ve dış paydaşlarla en üst düzeyde ele alınması ve güvenlik sıkılaştırmalarının düzenli olarak yapılması,

d) Taşra teşkilatının merkez teşkilatı ile iletişim altyapısının güçlendirilmesi.

3. SOSYAL GÜVENLİK KURUMUNDAKİ SİBER GÜVENLİK UYGULAMALARI VE POLİTİKALARI

SGK'nın siber uzayda sunduğu hizmetlerin her geçen gün artması, bu hizmetlerin, varlıkların ve sistemlerin güvenliğinin sağlanmasına yönelik çalışmalara da hız kazandırmıştır. Bu amaç doğrultusunda Kurum Bilgi Teknolojileri Servis Yönetimi ve Stratejik Güvenlik Uygulaması konularında Teknik Destek ve Eğitim Hizmeti satın alınmıştır. Bu hizmet ile ISO 20000 ve ISO 27001 belgeleri alınmış, bu şekilde Kurumun çok daha güvenli ve etkili yönetilebilir bir bilgi teknolojileri altyapısına kavuşması, Kurumun vatandaşlara sunduğu servislerin kalitesinin fark edilebilir derecede artması ile yüksek kalitede ve güvenli hizmetlerin sunulmasını destekleyen hedeflerinin gerçekleşmesi sağlanmıştır (SGK, 2013b:154).

SGK'nın ISO 20000 belgesi ile ISO 27001 belgesine sahip olması, siber güvenliğin sağlanması için önemli olan Güvenlik Politikaları Uygulaması, Bilgi Güvenliği Organizasyonu Uygulaması, İnsan Kaynakları Güvenliği Uygulaması, Varlık Yönetimi Uygulaması, Erişim Kontrolü Uygulaması, Fiziksel ve Çevresel Güvenlik Uygulaması, Operasyon Güvenliği Uygulaması, İletişim Güvenliği Uygulaması, Sistem Edinim, Geliştirme ve Bakım Uygulaması, Tedarikçi İlişkileri Uygulaması, Bilgi Güvenliği Olay Yönetimi Uygulaması, Bilgi Güvenliği Açısından İş Sürekliliği Yönetimi Uygulaması ve son olarak da Uyum Uygulaması konularında çalışmalar yapıldığının göstergesidir (bilgiguvenliginotlari.com, 2014). Bu uygulamalar ile ulaşılmak istenen şey siber güvenliğin hedefleri arasından olan gizlilik, bütünlük ve erişilebilirliğin sağlanmasıdır. Bu çerçevede, kurumun söz konusu belgelere sahip olması yukarıda saydığımız konularda denetimlerden geçerek standartları sağladığının ve dolayısıyla bu belgeyi almaya hak kazandığının göstergesidir. ISO 20000 ve ISO 27001 belgeleri her ne kadar bilgi güvenliği yönetim sistemine dair standartların sağlandığını gösterir belge olsa da, bu standartların siber güvenliğin sağlanmasında da önemli olduğu açıktır.

Bu bölümün devamında SGK'nın siber güvenlik bağlamındaki uygulamaları ve politikaları anlatılacaktır.

3.1. Merkez ve Taşra Bilgi İşlem Altyapısının Güçlendirilmesi

SGK'nın merkez ve taşra teşkilatlarının donanım yenilemeleri, kurumsal donanım, ağ ve iletişim altyapılarının modernize edilmesi işlemleri yapılmıştır. Kurumun

bilişim teknolojileri ekipmanlarının geliştirilmesine yönelik çalışmalar gerçekleştirilmiştir. Bununla birlikte donanım, işletim sistemleri ve uygulamalarının sürüm yükseltme çalışmaları da tamamlanmıştır. Söz konusu bu çalışmalar teknolojik gelişmeler ile daha koordine ve verimli olarak kullanılacaktır (SGK, 2012:39-40). Bilişim altyapısının modernize edilmesi kurumsal kaynak planlamalarının etkin yönetilmesini sağlamaktadır. Siber güvenlik sadece yazılım düzeyinde ele alınan bir kavram olmayıp bütünsel bir yaklaşımın ortaya konmasını, güçlü bir donanım ve ağ yapısıyla sistemin desteklenmesini gerektirmektedir. Bu anlamda siber güvenlik kapsamında güvenliğin bir parçası olan donanım ve ağ altyapısının modern yapıya kavuşturulması siber güvenlik teknolojilerinin uygulama düzeyini artırmaktadır.

3.2. Erişim Kontrolleri İle İlgili Uygulamaları

Siber güvenliğin sağlanması adına erişim kontrol uygulaması ile ilgili olarak, "Kullanıcı Taahhütnameleri" hazırlanmıştır. Bu çerçevede sisteme erişim sağlayacak personel bu taahhütnamede belirtilen gizlilik politikaları ve şartlara göre sistemi kullanacağını taahhüt ettikten sonra sistemi kullanabilmektedir. Kimlik Paylaşım Sistemi Kullanıcı Taahhütnamesi, Kurum Çalışanları Politika Bilgi Güvenliği Taahhütnamesi, Üçüncü Taraf Çalışanları Politika Bilgi Güvenliği Taahhütnamesi, Gizlilik Anlaşmaları, Bilgi Güvenliği Kuralları söz konusudur. Kurum sistemlerine erişim için yetkilendirme kuralları belirlenmiştir.

Bir diğer erişim kontrol uygulaması, biyometrik kimlik doğrulama yöntemleri arasında yer alan Avuç İçi Damar İzi Okuma Sistemi ve Parmak Damar İzi Tarama Yöntemi ile ilgili çalışmalar yapılmıştır.

Kurumun sistemlere sadece erişim yetkisi olanaklarının sağlanması adına işi tek elde toplayan merkezi yetki birimi oluşturulmuş ve bu birim tarafından sistemlere erişim talepleri değerlendirilmekte ve yetkilendirme işlemlerini yapılmaktadır.

Kullanıcı girişi ve yetkileri geniş bir yelpazede hizmet sunan kurumlar için çok önemli hale gelmektedir. Özellikle de dışa açık sistemlerde siber saldırıların en çok bu noktaları tercih ettiği, yani kullanıcı bilgileri kullanılarak sistemlere normal erişimlerin sağlandığı, bu konuda çok fazla bilgi işlem ihlallerinin yaşandığı görülmektedir.

Kamu kurumlarının iç kullanıcıların şifrelerinin içerideki birden fazla personel tarafından bilinmesi, yetki düzeyinde yaşanan karmaşa, uzun süreli log kayıtlarının tutulmaması, bazı uygulamalarda yapılan işlemelerin kayıtlarının tutulmaması sürekli eleştiri konusu olmakta, bu konuda yapılacak araştırmalarda sonuca ulaşmayı imkânsızlaştırmaktadır.

Dünya genelinde yaşanan kurumsal bilgi sızmalarının çoğunda içeriden bir desteğin olduğu bilinmektedir. Bu sızmalarda kullanıcı bilgilerine erişildikten sonra saldırı uzun süre fark edilmeyebilmektedir. Çünkü kurumsal düzeyde kullanıcı davranışlarına yönelik analizler yapılmamaktadır. Dış kullanıcılar içinde bu tür ele geçirmeler ve kullanımlar söz konusu olmaktadır.

Burada kullanıcıların kimlik bilgilerinin ele geçirilmesi, kişilerin son kullanıcı olması durumunda ve uygulamaların doğrudan veri tabanından bilgiyi son

kullanıcının ekranına göndermemesi durumunda elde edilen bilgiler yetki düzeyiyle sınırlı kalmakla birlikte, kişinin sistem sorumlusu olup veritabanı, güvenlik, ağ yöneticisi gibi yetkileri bulunması durumunda ve bu kişilerin erişimlerinin güvenlik düzeyinin dışarıdan erişim için düşük olması durumunda işin tehlikesi çok daha büyük olmaktadır.

Sistem yöneticilerinin erişim şekillerindeki zaafiyet kurumları çok büyük tehlikelere maruz bırakabilmektedir. Yine son kullanıcının yetkilerinin saldırganların ellerinde güçlü bir araç olarak kullanılabileceği unutulmamalıdır. Örneğin, SGK sağlık hizmeti sunan bir kurumdur. Son kullanıcı olan bir eczane ya da hastane toplumun önde gelen kişilerin sağlık verilerine ulaşmaktadır. Kişinin kanser hastası, HIV vb. olduğu bilgisinin kişinin aleyhine kullanımının önlenmesi için bu bilginin sadece ilgilileri tarafından bilinmesi ve bu bilgilere bakan kullanıcıların log kayıtlarının soruşturulmaya elverişli ve güvenilir şekilde tutulması çok önemlidir.

3.3. Fiziksel ve Çevresel Güvenliğin Sağlanması İle İlgili Uygulamalar

Bu güvenlik uygulamasında amaç, işyerlerine yetkisiz erişimlerin engellenmesi ve bilgi bağlamındaki varlıkların tehlikelere ve çalınmaya karşı muhafaza edilmesidir. Bu doğrultuda SGK'da son yıllarda fiziksel sunucu sayısı azaltılmıştır, bu şekilde sunucuların bakımı ve güvenliğinin sağlanması daha kolay yapılacaktır.

3.4. Yedekleme Uygulaması

SGK çok fazla veri toplayan ve bunu işleyen bir kamu kurumudur. Bu verilerin bir kısmı 7/24 sürekli kullanımdadır. Verilerin toplanması ve işlenmesi kadar yedeklenmesi de büyük önem taşımaktadır. SGK, çok fazla veriyi toplamakla birlikte bu verileri uzun süre saklamak ve her an kullanıma hazır halde tutmak zorundadır. Bu verilerin yedeklenmesi siber saldırı durumunda sistemin sürekliliğinin sağlanması açısından çok önemlidir. Kurumda yedekleme uygulaması adına farklı uygulamaların çalıştığı çeşitli sunucuların merkezi sunucular üzerine yedeklerinin alınması işlemleri yapılmaktadır. Ayrıca da merkezi sistem oluşturulması adına felaket kurtarma merkezleri oluşturulmuştur.

3.5. Veri Tabanı İşlemleri İle İlgili Uygulamalar

SGK iki ayrı bilgi işlem merkezinden oluşan ağ (network) altyapısına sahip olup, bunlar Mamak ve Kızılay Bilgi İşlem Merkezleri olmak üzere Kurumun Geniş Ağ Alanı (WAN) bağlantılarının sonlandırıldığı yerleşkelerdir (SGK, 2013a:18). Veri Merkezi Projesi ile Kurumun gelecekteki en az 15-20 senelik bilgi sistemleri ihtiyacını karşılayacak kapasitede ve teknolojide, Ankara/Batıkent'te 58 dönümlük bir arsa üzerinde SGK Veri Merkezi inşa edilecektir. Proje tamamlandığında; Türkiye'nin en büyük sanallaştırma altyapısı kurularak vatandaşlara ve diğer paydaşlara 7/24 kesintisiz hizmet sunulacaktır (SGK, 2013b:153).

Halihazırda SGK, bilinen internet altyapısı üzerinden hizmet vermektedir. Bu durumun şüphesiz güvenlik zaafları olacaktır. SGK, internet üzerinden gelebilecek bu güvenlik zaaflarını ortadan kaldırmak için bilgi işlem merkezi ile hizmet noktaları arasında internetten bağımsız sadece Kuruma has kapalı devre bir iletişim altyapısı kurmayı hedeflemiştir. Bu şekilde, izlenebilen, yedekli ve güvenli bir sistem kurulmuş olacaktır.

SGK ağ yapısının herkesin kullandığı internet altyapısı üzerinden hizmet vermesi, siber saldırılar yönüyle kolay hedef olmasını sağlamaktadır. Kamu kurumlarının siber uzaydan gelebilecek saldırıları karşı bu amaçla aldığı önlemlerden birisi iç ağ ve dış ağ sistemlerini ayrı bir biçimde oluşturmaktır. Adalet Bakanlığı'nın UYAP, Emniyet Genel Müdürlüğü'nün POLNET, Sayıştay'ın SAYBİS, SGK'nın sgk.intra sistemi bu amaçla oluşturulan uygulamalardır.

Üstelik bu saldırılarda doğrudan hedef tespiti zorlaşmakta, ağlar saldırılar sırasında yavaşlamakta ve saldırılar sırasında sistemin tamamen veya kısmen kapatılması gibi durumlar ortaya çıkmaktadır.

3.6. Veri Ambarı ve Veri Madenciliği

SSK, Bağ-KUR ve Emekli Sandığı'nın birleştirilmesiyle ile oluşturulan tek çatı, istatistiki bilgi ve raporların tek noktadan oluşturulmasını zorlaştırmıştır. Bu sorunu aşmak amacıyla 2008 yılında başlatılan Veri Ambarı Projesi, 2009 yılında faaliyete geçmiştir ve bu şekilde kurum verileri tek bir veri tabanında birleştirilmiştir.

Veri ambarı, Kurum birimlerine;

- Risklerin önceden görülmesi,

- Denetim ve kalitenin sağlanması,

- Dinamikliğin sağlanması,

- Taktik geliştirilmesi,

- Kaçak yakalama altyapısının oluşturulması,

- Risk odaklı sağlık ve sosyal sigorta denetimlerine raporlar sunulması,

- Kamu kurumları ile ortak veri ambarlarının oluşturulması,

- Aktüeryal denge analizi yapmak üzere istatistiki veri oluşturması fonksiyonlarında katkı sağlamaktadır (SGK, 2012:43-44).

Ayrıca SGK veri madenciliği açısından mevcut sistemin geliştirilmesi ile Kurumun en önemli faaliyet alanlarından olan sağlık alanındaki usulsüzlüklerin tespitine yardımcı olunması ve kayıt dışı istihdamın önlenmesi adına çalışmalar yapmaktadır (SGK, 2012:44).

Veri madenciliği bağlamında Kurumun hedefleri şunlardır (SGK, 2012:44);

* Halihazırdaki veri ambarı sisteminin altyapısını ve yeni projeleri de düşünülerek geliştirilmesi,

* Mevcut veriler daha çok işlenerek kullanıcılara daha çok sorgulama alanlarının oluşturulması,

* Bu şekilde Kuruma klasik yollarla gelen bilgi taleplerinin azaltılması; iş gücü ve zamandan tasarruf edilmesi,

* Kurumda meydana gelen ihtilafların sistem üzerinden izlenilmesi ve daha hızlı sonuca gidilmesi,

* Merkez ve taşra teşkilatlarından gelen bilgi taleplerinin hızlı bir şekilde yerine getirilmesi,

* Büyük çaplı veri mimari altyapısının temellerinin oluşturulması.

3.7. Güvenlik Politikaları Uygulaması

SGK tarafından bilgi güvenliğinin ve siber güvenliğin sağlanması adına kurum ile ilgili olarak e-posta kullanım ve yönetim politikası, şifre politikası, temiz masa/temiz eller prensipleri ve bilgi güvenliği politikaları belirlenmiştir. Kurum çalışanlarının bu prensibe uygun hareket etmesini beklemektedir. Belirlenen bu politikalarla ilgili olarak kullanıcı taahhütnameleri hazırlanarak kurum personelinin bu politikalara uygun hareket etmesi sağlanmaktadır (Sosyal Güvenlik Kurumu Hizmet Sunumu Genel Müdürlüğü, 2011:50-51).

Bilgi güvenliğinde kullanıcının belirlenen politikalara uygun hareket etmesi beklentisinden öte kullanıcıların bu alanların dışına çıkamamaları esastır. Çok kullanıcılı bir yapı, yetki ve görevlerin çok hızlı değişmesi gibi durumlar kamu kurumlarında bilgi işlem yönetimini oldukça zorlayan konular arasındadır. Kullanıcıların yetkileri verilirken, değiştirilirken ve alınırken işleyişin yavaş olması bilgi güvenliği ihlallerine sebep olmaktadır. Kişiye yetki verilip daha sonradan kullanıcı taahhütnamesi imzalatılması, kurumdan ayrılmış bir kişinin e-postasının hala aktif olması gibi sorunlarla sıklıkla karşılaşılmaktadır.

3.8. E-SGK Uygulamaları

SGK'nın internet üzerinden vatandaşların hizmetine sunduğu E-SGK uygulamalarını siber güvenlik bağlamında incelemek ve değerlendirmek gerekmektedir.

Vatandaşlar SGK'nın bu mobil uygulamalarına http://www.sgk.gov.tr/wps/portal/tr/e_sgk adresinden erişebilmektedir.

Şekil 1: E-SGK Uygulamaları

Kaynak: SGK, 2015c.

E-SGK uygulamalarından bazıları ve bunlara ulaşmak için istenen bilgiler aşağıdadır:

1. E-Bildirge uygulamasında işverenlerden kullanıcı adı, sistem şifresi ve işyeri şifresi istenmektedir. Bu şekilde işverenlerin aylık prim ve hizmet belgelerini internet üzerinden göndermeleri sağlanmaktadır.

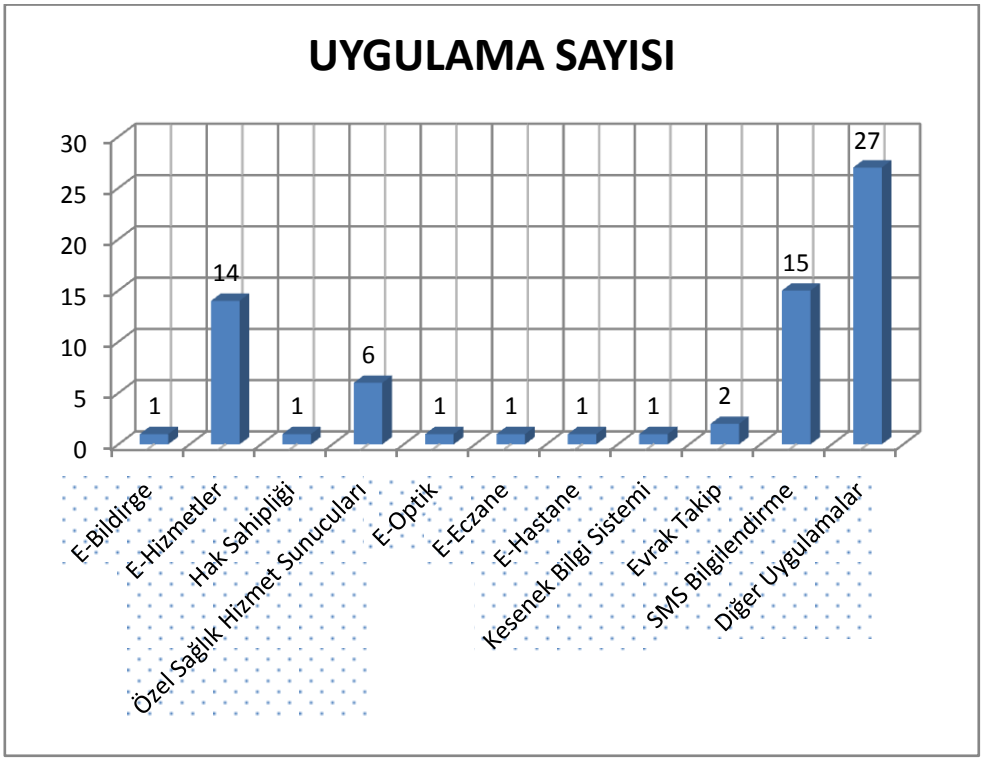
2. E-Hizmetler uygulamasında vatandaşlardan TC Kimlik Numarası, İl, Doğum Yılı ve Cilt Numarası istenmektedir. Eğer insanlar bu bilgileri girebildiyse; bilgileri girilen kişinin 4A (SSK), 4B (Bağ-KUR) ve 4C (Emekli Sandığı) tescil kaydı ve emekli aylığı bilgilerine, 4A ve 4B hizmet bilgilerine, 4A ve 4B iş göremezlik ödeme bilgilerine ve sağlık provizyon gibi bilgilerine ulaşılması mümkündür.

3. Evrak Kayıt uygulamasında vatandaşlardan sadece TC Kimlik Numarası istendiği görülmektedir. TC Kimlik Numarası girilen kişinin son 6 yıl içerisindeki SGK ile ilgili olan evraklarının takibi yapılabilmektedir.

4. SMS Bilgilendirme uygulamasında vatandaşlardan TC Kimlik Numarası ve Aile Sıra Numarası istenmektedir.

5. Diğer uygulamalardan turkiye.gov.tr'ye yönlendirilip e-devlet şifresi isteyenler olduğu gibi kullanıcı adı ve parola bilgisi isteyenler de bulunmaktadır.

Şekil 2: E-SGK Portalındaki Uygulama Sayıları



Kaynak: SGK, 2015c'den derlenmiştir.

Tablo 1: E-SGK Uygulamalarına Erişimde İstenen Bilgiler

Uygulama	Kullanıcı Adı ve Şifresi	E-Devlet	Nüfus Cüzdanı Bilgileri	TC Kimlik No
E-Bildirge	+			
E-Hizmetler			+	+
Hak Sahipliği				+
Özel Sağlık Hizmet Sunucuları		+		
E-Optik	+			
E-Eczane	+			
E-Hastane	+			
Kesenek	+			

Bilgi Sistemi				
Evrak Takip				+
SMS Bilgilendirme			+	+
Diğer Uygulamalar	+	+		

Kaynak: SGK, 2015c'den derlenmiştir.

E-SGK uygulamaları içerisinde yaklaşık 70 adet uygulamanın olduğu, bu uygulamalarda erişim yetkilerinin başlıca dört şekilde gruplandığı; SGK tarafından verilen "Kullanıcı Adı ve Şifresi" ile erişim, E-Devlet sistemi üzerinden erişim, Nüfus Cüzdanı Bilgileri ile erişim ve T.C. Kimlik No ile erişim yapılabildiği görülmektedir.

Kurumun kendisine veri girişi istediği durumlarda doğrudan bilgi girişini yapmak istediği kişilere güvenlik standartlarına uygun kullanıcı adı ve şifre girişi ekranı oluşturması doğru bir yaklaşım olarak değerlendirilebilmektedir.

Ancak veritabanında yer alan kişisel bilgilerin; kişilerin taşınabilir ve çoğu işlemde paylaşılabilir (örneğin kredi çekerken alınan kimlik fotokopisi) olarak kullandığı nüfus cüzdanı bilgileriyle erişilebilir hale getirilmesi bilgi güvenliği ihlalidir. Üstelik Kurum "1 - Sosyal Güvenlik Bilgilerinizin www.sgk.gov.tr web sayfasında görüntülenmemesi yönünde bir talebiniz mevcut ise, Sosyal Güvenlik İl Müdürlükleri veya Sosyal Güvenlik Merkezlerine Şahsen Dilekçe ile başvurabilirsiniz. Kişisel bilgide önce yayınlanma izni alınmalıdır. Kısıtlama talebi bilgi çıktıktan sonra bir işe yaramaz." uyarısıyla bilgiyi öncelikle erişilebilir kılma yöntemi tercih etmiştir. Halbuki kişisel bilginin önce korunması ve gizlenmesi tercih edilmelidir. Vatandaşın bunu basit yöntemlerle erişeme izin vermesi yöntemi tercih edilmelidir.

Evrak Kayıt uygulamasında yine kişi TC Kimlik Numarasıyla adına işlem gören bir evrakı sorgulayabilmektedir. Burada örneğin bir şikayet üzerine denetimi yapılan işveren çalışanlarının SGK'da evrak kaydı olup olmadığını TC kimlik Numarasıyla sorgulayarak şikayet edeni öğrenebilir.

E-SGK uygulamalarından SMS Uygulamaları sisteminde operatörlerin mesaj kayıtlarının bir kopyasının tutulması riskinin ortadan kaldırılması önemlidir.

Sistemde paylaşılan bilgiler e-devlet üzerinden paylaşılmalı ya da e-devlette uygulanan e-imza, mobil imza, geçilmesi planlanan elektronik kart gibi daha güvenlikli sistemler üzerinden erişilebilir kılınmalıdır. E-devlet üzerinden yapılan paylaşımlar web servisler yoluyla özellikle veritabanına doğrudan erişimi engelleyecektir. Bu siber saldırılar için daha zor bir duvar olacaktır. Yine çok fazla uygulama geliştirilmesine bağlı olarak gözden kaçacak güvenlik tedbirleri ortadan kalkacaktır. Bu arada yatırım maliyeti azalacaktır. Çünkü kurumların e-devlet hizmetlerini zaten e-devlet sistemine taşımaları gerekmektedir. Böylece ikinci bir yatırım ortadan kalkacaktır. Tüm kurumların e-devlet üzerinden erişim sağladığı

yapılarda daha güncel güvenlik tedbirleri alınması sağlanabilecektir. Ani saldırılarda da tüm kurumlara erişimi tek noktadan önleme gerçekleşebilecektir.

SONUÇ VE DEĞERLENDİRME

Bilişim sistemleri ve ileri teknolojiler insanların yaşamlarını kolaylaştıran araçlar olarak kurumların ve bireylerin hayatına gün geçtikçe daha çok girmektedir. Bununla beraber siber tehditlerinin çeşitleri ve sayıları da artmaktadır. Siber alanda oluşan bu risk ve tehditlere karşı politikalar ve stratejiler geliştirmek ve bunları güncel tutmak gerekmektedir.

Artık herhangi bir kuruma bir işlem için gidildiğinde işlemi gerçekleştiren memur mutlaka kurumun bilişim altyapısını kullanmakta hatta insanlar kurum binalarına gitmeden de internetten şifreleriyle ya da şifresiz yapmak istedikleri işlemleri gerçekleştirebilmektedir.

Bakır, siber güvenlik kavramının iyi kavranılması gerektiği üzerinde durmakta ve şu önerilerde bulunmaktadır (2012:15):

* Mevzuat altyapısının düzenlenmesi,

* Uluslararası hukuk bağlamındaki haklar adına hazırlık yapılması,

* Ulusal bilgisayar olaylarına müdahale anlamında gerekli organizasyonların oluşturulması,

* Ülkenin siber güvenlik altyapısının güçlendirilmesi,

* Siber güvenlik alanında uzman yetiştirilmesi,

* Siber güvenlik alanında ulusal teknolojilerin geliştirilmesi.

Buradan yola çıkarak SGK'nın hizmet verdiği vatandaş sayısı ve bilişim altyapısı göz önüne alındığında siber güvenlik uygulamaları ve politikalarıyla ilgili şu tespit, değerlendirme ve öneriler yapılabilir;

- Kurumsal bilgi güvenliği politikalarının belirlendiği, ancak bu politikalardan çalışanların tamamının haberdar olmadığı görülmektedir. Bilgi güvenliği politikalarının belirlenmiş olmasının yeterli değildir; aynı zamanda bunların tüm çalışanlara duyurulması ve sorumluluklarının neler olduğunun öğretilmesi gerekmektedir.

- Kurumda görev, rol ve sorumluluk tanımlamaları tam anlamıyla yapılması gerekmektedir. Siber alanda gerçekleştirilecek iş ve işlemlerden kimin sorumlu olacağı, görev ve yetkileri ortaya koyacak mevzuat dokümanlarını oluşturmak gerekmektedir.

- SGK bilişim sistemlerinin siber güvenliğinin sağlanmasında kullanmış olduğu yazılımların yerli ürün olması ayrıca önemlidir. SGK, iç ve dış paydaşlar için sunmuş olduğu hizmetlere ait yazılımları kendisinin üretmesinde fayda bulunmaktadır.

- SGK'nın siber güvenlik stratejisini Ulusal Siber Güvenlik Eylem Planları çerçevesinde oluşturmak gerekmektedir.

- Siber güvenliğin bir bütün olduğunu düşünürsek, hem iç paydaşlar hem de dış paydaşların da konudan haberdar edilmesi, onlara yönelik de farkındalık eğitimleri verilmesi gerekmektedir.

- İnternet üzerinden gelebilecek siber saldırıları önlemek adına Kurumun iç ağ sistemiyle dış ağ sistemi olan internet ağının birbirinden ayrılması gerekmektedir.

- Kurumun farklı birimlerinde farklı güncel virüs yazılımlarının kullanılmasının sağlanması gerekmektedir.

- E-SGK uygulamalarında kişilerin rızası olmadan bilgileri erişime açılmaması ve e-devlet şifresiyle girişin altyapısının oluşturulması gereklidir.

- SGK'nın bilgi işlem altyapısında oluşabilecek herhangi bir sorun neticesinde meydana gelecek maddi ve manevi maliyetler göz önüne alındığında Kurum bilgi işlem ve siber güvenlik sisteminin önemi bir kez daha ortaya çıkmaktadır.

KAYNAKÇA

Bakır, Emre. (2012), "Türkiye'de Siber Güvenlik", *Bilim ve Teknik Dergisi*, Yıl:46, S.540, s.12-15.

Bakır, Emre. (2014), "Siber Savaşlar-Başlangıç", http://www.siberguvenlik.org.tr/2012/12/siber-savaslar-baslangc.html, (Erişim Tarihi: 14.08.2014).

Bilgi Güvenliği Derneği. (2012), "Ulusal Siber Güvenlik Stratejisi", http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf, (Erişim Tarihi: 12.01.2015).

bilgiguvenliginotlari.com. (2014), "ISO 27001: 2013 ve ISO 27002: 2013 Standartları Yayınlandı", http://www.bilgiguvenliginotlari.com/blog/2013/12/12/iso-270012013-ve-iso-270022013-standartlari-yayinlandi/, (Erişim Tarihi: 12.01.2015).

Bilgi Teknolojileri ve İletişim Kurumu. (2014), "Genel Bilgi", http://btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php, (Erişim Tarihi: 10.11.2014).

Clarke, Richard A. ve Knake, Robert K. (2010), *Cyber War: The Next Threat to National Security and What to Do About It*, 1. Baskı, HarperCollins Publishers Ltd, New York.

Çifci, Hasan. (2013), *Her Yönüyle Siber Savaş*, 1. Baskı, TUBİTAK Popüler Bilim Yayınları, Ankara.

Ege, Börteçin. (2012), "Siber Savaşlar - Bilişimin Karanlık Yüzü", *Bilim ve Teknik Dergisi*, Yıl:46, S.540, s.18-22.

Hekim, Hakan ve Başıbüyük Oğuzhan. (2013), "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, C.4, S.2, s.135-158.

Kaya, Adem. (2012), *Siber Güvenliğin Milli Güvenlik Açısından Önemi*, T.C. Kara Harp Okulu Savunma Bilimleri Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, Ankara.

Sosyal Güvenlik Kurumu Hizmet Sunumu Genel Müdürlüğü, (2011), *Hizmet Sunumu Genel Müdürlüğü İş ve İşlemleri konulu 2011/23 sayılı Genelge*.

SGK. (2012), "Sosyal Güvenlik Reformu Sürecinde Yapılan Faaliyetler ve Devam Eden Projelerimiz", http://www.sgk.gov.tr/wps/wcm/connect/602b93a7-7a4c-4954-b474-1f491e8ee81b/SGKFaaliyetler08082012_yeni.pdf?MOD=AJPERES, (Erişim Tarihi: 26.12.2014).

SGK, (2013a), 2013 Yılı Faaliyet Raporu.

SGK, (2013b), "Sosyal Güvenlik Reformunun 4. Yılında 400 Yenilik", Yayın No:80, http://www.sgk.gov.tr/yayinlar/01_SGK-400_yenilik.pdf, (Erişim Tarihi: 20.02.2015).

SGK, (2014a), "Sosyal Güvenlik Kurumu 2014 Yılı Performans Programı", http://www.sgk.gov.tr/wps/wcm/connect/8b5fbd55-8d64-423b-abd4-e768221ef524/duyuru_20140212_07.pdf?MOD=AJPERES&CACHEID=8b5fbd55-8d64-423b-abd4-e768221ef524, (Erişim Tarihi: 20.02.2015).

SGK, (2014b), "Sosyal Güvenlik Kurumu Unvan Bazında İş Görev Tanımları Kitabı", http://www.sgk.gov.tr/wps/wcm/connect/e82dcd35-1f4e-49f9-9927-567fac013f62/unvan_bazinda_is_gorev_tanimlari_kitabi_2014-14.pdf?MOD=AJPERES, (Erişim Tarihi: 20.02.2015).

SGK, (2015a), "Hizmet Sunumu Genel Müdürlüğü/Hakkımızda", www.sgk.gov.tr, (Erişim Tarihi: 20.02.2015).

SGK, (2015b), "Hizmet Sunumu Genel Müdürlüğü/Organizasyon Yapısı", www.sgk.gov.tr, (Erişim Tarihi: 20.02.2015).

SGK, (2015c), "Mobil Uygulamalar", http://www.sgk.gov.tr/wps/portal/tr/e_sgk, (Erişim Tarihi: 14.01.2015).

Storch, Tyson. (2012), "Siber Güvenlik: Güvenli ve Bağlantılı Bir Toplumun Temel Taşı", http://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBsQFjAA&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F9%2F0%2F9%2F90945F31-C24F-4E68-8A23-D35E74093CDD%2FTrustworthy%2520Computing%2520Cybersecurity%2520white%2520paper_TR.pdf&ei=7AK0VPyPI-mc7Aa7goGwBA&usg=AFQjCNH81XBNsU43Y58xbJUtVojibYnqcg, (Erişim Tarihi: 12.01.2015).

United State DoD. (2006), "The National Military Strategy for Cyberspace Operations", http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf, (Erişim Tarihi: 12.01.2015).

United State DoD. (2010), "Departmant of Defence Dictionary of Military and Associated Terms", http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (Erişim Tarihi: 12.01.2015).

Ünver, Mustafa, Canbay, Cafer ve Mirzaoğlu, Ayşe Gül. (2009), *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*, Bilgi Teknolojileri ve Kurumu Başkanlığı, Ankara.

Ünver, Mustafa ve Canbay, Cafer. (2010), "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", *Elektrik Mühendisliği*, S.438 (Mart), s.94-103.

White House. (2003), "The National Strategy to Secure Cyberspace", https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (Erişim Tarihi: 12.01.2015).

5502 Sayılı Sosyal Güvenlik Kurumu Kanunu.