YAZILIM GÜVENLİK AÇIĞI EKOSİSTEMİ VE TÜRKİYE'DEKİ DURUM DEĞERLENDİRMESİ

Oğuz BOZOKLU[1] ve **Celal Zaim ÇİL**[2]
[1]ODTÜ Fen Bilimleri Enstitüsü, Çankaya, Ankara,
[2]Empinovas Ltd. Büklüm Sok. No. 6 D.11 Kavaklıdere, Çankaya, Ankara,
obozoklu@gmail.com, czaimcil@empinovas.com

ÖZET

Günümüzde ticari yazılımlar, özellikle internet tarayıcıları ve işletim sistemleri, hem kaynak kodu bakımından çok büyüktür, hem de kamu ve özel sektör tarafından yaygın olarak kullanılmaktadır. Bu ve benzeri diğer yazılımlara ait yazılım güvenlik açıklarının tespiti, raporlanması, açık için yama üretimi, yama yönetimi vb. faaliyetler önem kazanmıştır. Bu açıklara ilişkin bilgilerin derlenmesi, tasnifi ve bir veri tabanı içinde tutularak düzen içinde kullanıma sunulması siber güvenliği artırmakta, açıkların istismarını ise zorlaştırmaktadır. Bu makalede yazılım güvenlik açığı ekosistemi, bu alandaki standartları büyük oranda belirleyen ABD başta olmak üzere dünyadaki diğer örnekleri ile bir literatür taraması yapılarak incelenmekte ve irdelenmekte, Türkiye özelindeki mevcut durum değerlendirilerek yerel yapıya dair özgün bir model önerilmektedir. Benzer bir çalışmanın ülkemiz için bugüne kadar yapılmadığı düşünülmektedir.

Anahtar Sözcükler: Yazılım güvenlik açığı, siber güvenlik, yazılım açığı veri tabanı, siber olaylara müdahale ekibi, güvenlik açığı yönetim modeli.

LITERATURE REVIEW ON SOFTWARE VULNERABILITY ECOSYSTEM AND TURKEY'S POSTURE

ABSTRACT

Today, commercial software, especially web browsers and operating systems have large source codes and at the same time have been widely used by the public and private sectors. It has been vital to discover the vulnerabilities of those software, reporting and patch them. Activities like classification, sorting and utilizing the vulnerability information via databases help to improve cyber security and decrease the probability of exploitation. This study reviews security vulnerability ecosystem with samples from the world, evaluates Turkey's status and recommends a unique model respectively. As far as we know, no other study of this kind has been made so far for Turkey's case.

Keywords: Software security vulnerability, cyber security, software vulnerability database, cyber incident response team, vulnerability management model.

1. GİRİŞ

Stuxnet, muhtemelen tarihteki, fiziksel etkisi doğrudan görülebilen ilk 'ciddi' siber saldırı olarak kayıtlara geçecektir. Dört adet Windows© güvenlik açığı ve iki çalıntı güvenlik sertifikası ile İran'da bulunan Natanz Uranyum Zenginleştirme Tesisindeki 984 adet SIEMENS marka santrifüjü hedef alan ve işlemez hale getiren bu saldırı, 500 kilobayt büyüklüğünde bir istismar dosyası ile yapılmıştır [1]. Yazılım güvenlik açıklarının bir mühimmat gibi, istismar kodlarının ise tek kullanımlık bir silah gibi kritik altyapılara karşı saldırı maksadıyla kullanıldığı "bilinen" en çarpıcı örnektir [2]. Bu konuda önde gelen araştırmacılardan Langner'e göre Programlanabilir Mantıksal Denetleyicinin (Programmable Logic Controller, PLC) istismar edilebilmesi için dört satırlık bir kod parçası yeterli olmaktadır [3,4].

Kritik altyapılarda ilk zamanlarda kullanılan, herkesin çok fazla bilgi ve fikir sahibi olmadığı özelleştirilmiş SCADA çözümlerinin yerini son dönemlerde kullanım kolaylığı ve ucuzluğu nedeniyle Windows ve UNIX gibi işletim sistemleri almaya başlamıştır [5,6].

Çok muhtemeldir ki büyük ticari yazılım üreticileri başlangıçta, ürünlerinin kritik sistemlerde yaygın olarak kullanılacağını hesaba katmamışlardı. Hızlı bir şekilde ve düşük maliyet hedefiyle geliştirdikleri ve daha çok sıradan kullanıcılar tarafından tercih edilen bu tür yazılımlar, zaman içerisinde askerî silah platformları, bankacılık ve finans ağlarında da kullanılmaya ve yaygınlaşmaya başlamışlardır [7].

Özellikle enerji sektöründeki "Akıllı Şebeke" (Smart Grid) projeleriyle İnternet üzerinden birbirine bağlanan kritik altyapılar, gün geçtikçe saldırıya daha açık bir hale gelmektedirler [7].

Yazılım güvenlik açığı[1]; bir yazılımın teknik özelliklerinde, geliştirmesi veya konfigürasyonu sırasında oluşan ve ortaya çıkması halinde yazılımın güvenlik politikasının örtük veya açık bir şekilde ihlaline neden olan kusur olarak tanımlanmaktadır [38].

Güvenlik açıklarının yoğunluğuna bakıldığında, ortalama bir yazılımın her 1000 satır kodunda yaklaşık 3 ilâ 20 arasında yazılım kusuru (bug) bulunduğu belirtilmektedir [8]. Bu bilgi, Tablo 1'deki verilerle birlikte değerlendirildiğinde, güvenlik açığı uzayının sınırlarına dair genel bir fikir edinilebilir. Buna ilave olarak, sistemlerin birçoğunun, farklı ülkelerde parça parça geliştirildiği de (tedarik zinciri güvenliği/zehirlenmesi) göz önüne alındığında, saldırganların güvenlik açığı ve kurban bulmakta zorlanmayacakları rahatlıkla söylenebilir [3].

Tablo 1: Kod Satır Sayıları [9,10].

Yazılım	Satır Sayısı (Milyon)
Mozilla Firefox	*9*
Google Chrome	*6,5*
MS Office 2013	*44,5*
F-35 JSF	*24*
Boeing-787	*14*

Gerek kritik altyapı ve tesislerin işlerliği ve devamlılığı, gerekse gündelik yaşamın aksaksız sürdürülebilmesi açısından siber güvenlik sadece teknik bir konu olmaktan çıkarak güvenlik stratejilerinin bir parçası haline gelmiştir.

İster saldırı, ister savunma, ister istihbarat adına olsun, siber uzayda atılan her adımın temelinde yazılım güvenlik açıkları ve bu açıkların istismarı yatmaktadır. Siber harekâtın (Stuxnet, Flame, Aurora vb.) etkin ve etkili olabilmesi için gerekli istismar kodlarının merkezinde bulunan bileşen ise güvenlik açıkları, özellikle de sıfırıncı gün (0-gün) açıklarıdır [11]. 0-gün açığı, herhangi bir yazılımda üreticisi dâhil hiç kimsenin istismar edilene kadar varlığından haberdar olmadığı bir yazılım güvenlik zafiyetidir.

Bu nedenle; güvenlik açıklarının tespiti, bilgilerin el değiştirmesi, alınıp satılması, duyurulması, raporlanması, güvenlik yamalarının üretilmesi yoluyla açığın kapatılması veya istismarı gibi konular, son derece detaylı bir şekilde ve ciddiyetle ele alınmalıdır.

Konuyla ilgili olarak, teknoloji öncüsü ülkelerde özellikle son yıllarda önemli birikim sağlanmıştır. Güvenlik açığı ekosistemi kapsamında bir takım kurumlar oluşmuş, pazarlar kurulmuş, ekonomisi ve kuralları büyük oranda ortaya çıkmıştır. Güvenlik açıklarının analizine olanak tanıyan, verinin standart formatlarda tutulduğu ve kamuoyu ile paylaşıldığı kapsamlı veritabanları bu maksatla yaratılarak kullanıma sunulmuştur.

Türkiye'de ise, siber güvenlik alanında ciddi atılımlar yapma niyeti dönemsel olarak ifade edilmekle birlikte, ortaya çıkan somut sonuçlara bakıldığında alınan mesafenin ve kamuoyu farkındalığının sınırlı kaldığı, uygulanabilir ve sürdürülebilir gayretler konusunda eksikler bulunduğu belirtilebilir

Genel hatları yukarıda çizilen çerçevedeki çalışmamızda sırasıyla; güvenlik açığı ekosistemindeki aktörler, süreçler ve yönetim usulleri, örnekler ve uygulamalar ile irdelenmekte, Türkiye'deki mevcut durum, güçlü ve zayıf yanları, geliştirilmesi gereken boyutlarıyla ortaya konulmakta, oluşturulması gereken yapıya dair örnek bir model önerilerek, değerlendirmeler bütüncül bir bakışla sunulmaktadır.

II. GÜVENLİK AÇIĞI EKOSİSTEMİ: AKTÖRLER, SÜREÇLER, YÖNTEMLER VE ARAÇLAR

Doğru bilginin, yerinde ve zamanında doğru kişinin elinde bulundurulması, geçmişten günümüze ihtiyaç duyulan ve önemsenen bir husustur. Siber güvenlik söz konusu olduğunda bilginin yönetimi ve zamanında paylaşılması daha fazla önem kazanmaktadır. Bazen dakikalar içerisinde olup biten saldırılar ve yerinde reaksiyon gösterildiğinde azaltılabilecek zararlar düşünüldüğünde, iyi planlama ve organizasyon ile farkındalığın her zaman üst düzeyde tutulması gerekmektedir.

[1]Makalede "yazılım güvenlik açıkları" yerine kısaca "güvenlik açığı" ifadesi kullanılmakta olup bu tabir, donanımsal güvenlik açığı, fiziksel güvenlik boşlukları ve/veya sosyal mühendislik gedikleri gibi boyutları içermemektedir. TDK Büyük Sözlük'te; *Açık: Bir gereksinimin karşılanamaması durumu. Açıklık: Boş ve geniş yer, meydanlık olarak* yer almaktadır.

Bu anlamda başlangıç seviye yeteneği veya temel bir girişim olarak değerlendirilebilecek CERT[2] veya Türkiye'deki ismiyle SOME[3] birimleri bulunmaktadır [12]. Yaşanan siber olaylara müdahale etmek ve ilgililer arasında bir iletişim ağı kurabilmek için birçok ülke ve kurumda bu tür ekipler oluşturulmuştur. Bunların ilklerinden biri olarak CERT/CC[4] (ABD), 1988 yılında, DARPA tarafından Carnegie Mellon Üniversitesinde kurulmuştur [13]. Hâlihazırda Dünya'da, CERT veya benzeri isim altında yaklaşık 350 organizasyon bulunmaktadır [14].

Güvenlik açıkları konusunda, bilgi paylaşımı ve koordinasyon büyük önem taşır. Küçük tedbirler ve önleyici bir takım hareketlerle çok büyük badireler engellenebilir veya etkisi azaltılabilir. Örnek vermek gerekirse; oltalama (phishing) saldırılarını tespit ve önleme sektöründe benzer işi yapan iki güvenlik firmasının, farklı bankalarla çalıştıkları bir dönemde karşılıklı olarak zamanında paylaşmadıkları bilgi nedeniyle yaklaşık 330 milyon dolar zarara uğradıkları sonradan anlaşılmıştır [1].

Güvenlik açıklarının yönetimi için sadece açığa ilişkin verilere sahip olmak da tek başına yeterli değildir. Bunun yanında; ne, nasıl ve ne şekilde sorularının cevaplarına dair bir birikim ve farkındalık gerekir. Bu noktada aşağıdaki gibi bir takım temel sorular akla gelmektedir.

Güvenlik açığı nedir? Bu açıklar nasıl tespit edilmektedir? Ne şekilde duyurulmaktadırlar? Geride duyurulmamış veya keşfedilmemiş ne kadar güvenlik açığı bulunmaktadır? Bunların duyurulmamış olması, keşfedilmedikleri anlamına gelir mi? Henüz keşfedilmemiş olmalarından yola çıkarak hiç olmadıkları sonucuna varılabilir mi?

Yukarıdaki soruların tamamına ayrıntısıyla cevap aramak ve bulmak bu çalışmanın sınırları ve kapsamı dışındadır. Ancak konuya dair farkındalığı artırmak, faydalı ve anlamlı yeni soruları akla getirmek için bu alandaki benzer çalışmaların artırılması ve derinleştirilmesinde fayda görülmektedir. Zira güvenlik açığı verileri büyük oranda dış kaynaklı ve çoğu zaman tek merkezli duyurulara ve konuyla ilgili "bilinenlere" dayanmaktadır. Bu konudaki varsayımlar ve eldeki bilgiler zaman zaman bulanıklaşabilmekte, hangi güvenlik açığı, ne kadar duyuruluyorsa o kadarını mı biliyoruz sorusu akıllara gelmektedir. Sıralanan gerekçelerle, güvenlik açığı ekosistemini, bu sistemdeki oyuncuları, süreçleri, kuralları ve konunun ekonomisini yakından tanımak adeta bir zorunluluk haline gelmiştir.

2.1. Aktörler: Paydaşlar

Güvenlik açığı ekosistemindeki temel aktörler; yazılım şirketleri, açığı bulanlar (açık avcıları), pazarlar, müşteriler, açığı duyuranlar (güvenlik haber kaynakları) ve düzenleyici organlar olarak sıralanmaktadır [15]. Geçtiğimiz yıllarda, yazılım güvenlik açıklarının ekonomik, askeri ve bilimsel değeri iyiden iyiye fark edilmeye başlanmıştır [11]. Bu nedenle devletin güvenlik ve istihbarat birimlerinin ve araştırmaları ile alana ışık tutan akademik çevrelerin de aktörler listesine ilave edilmesi gerekmektedir.

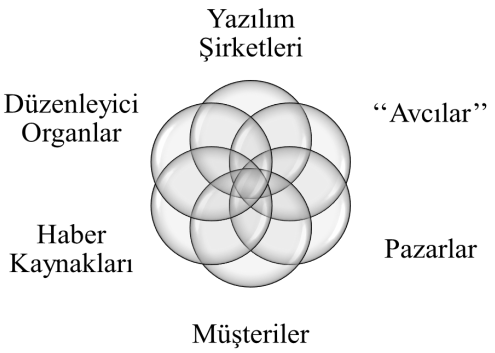
Şekil 1'de gösterildiği üzere bu konudaki sınıflandırmalar arasında bir geçişkenlikten bahsedilebilir. Aktörler ve roller arasındaki ilişkiler, keskin çizgilerle tanımlanmış değildir. Örneğin, güvenlik açığı konusunda kamuoyunu bilgilendiren bir kurum, aynı zamanda düzenleyici platformların bir üyesi olarak görülebilirken, bir yazılım şirketi açığın alıcısı veya bulucusu olarak, devlet istihbarat birimi ise açığın bulucusu, alıcısı veya kullanıcısı (istismar edeni) olarak süreçte rol alabilmektedir. Burada önemli olan, rollerin kapsamının ve içeriğinin iyi bir şekilde tanımlanması ve anlaşılmasıdır.

Yazılım Şirketleri

Yazılım şirketleri veya üreticiler, yazılımın geliştirilmesi safhasında güvenlik açığını yaratmaları sebebiyle, ileride yaşanması olası bir güvenlik zafiyetinin doğal sorumlusu olarak görülmektedirler. Yazılım geliştiriciler, projeyi bir an önce tamamlama güdüsüyle hareket etmekte, ancak pazarda baskın konuma gelmeye başladıklarında yazılım güvenliğini öncelikli bir konu olarak ele almaktadırlar. Zira yazılım şirketleri üzerindeki kamuoyu baskısı, daha hızlı yama yapmaları konusunda onları zorlamaktadır [16]. Yazılım geliştiriciler; şirketler, alt yükleniciler, bağımsız çalışanlar, tam zamanlı yazılım mühendisleri veya ortak geliştirme platformlarından (open community) oluşabilmektedir.

Destek sağlamakla sorumlu oldukları ürünlerde bulunan güvenlik açıklarını herkesten önce tespit etmek ve yamalar üretmek, yazılım şirketleri açısından itibarın korunması ve yasal yükümlülüklerin bir gereğidir. Bu maksatla yazılım şirketleri, güvenlik açığı bilgilerine erişebilecekleri her türlü yol ve yöntemi sistematik olarak takip etmektedirler. Piyasaya sunulmadan önce; deneme (alfa, beta vb.) sürümlerinden gelen geri beslemeler, şirket içi zafiyet analiz, tespit ve test ekipleri, yaygın kullanıma verme sonrası teşvik programları ve yarışmaları (bug bounties) ile pazarda yer almayı ve pazara yön vermeyi hedeflemektedirler.

[2] Cyber Emergency Response Team.
[3] Siber Olaylara Müdahale Ekibi.
[4] Bilgisayar Olaylarına Müdahale Koordinasyon Merkezi.



Şekil 1: Aktörler: Paydaşlar.

Ne var ki Microsoft, Google vb. büyük şirketlerin haricinde kalan orta ve küçük boy üreticilerin, bu tür pazarlarda etkin birer oyuncu olmaları zor görülmektedir. Hatta bazı yazılımların resmi bir temsilcisi veya üreticisi dahi bulunmamaktadır [15].

Güvenlik Açığı Avcıları: Açığı Tespit Edenler
Güvenlik açığı avcıları ya da "kâşifleri", yazılımlardaki güvenlik açıklarını bulmak için değişik motivasyonlarla çalışan insanlar olarak tanımlanmaktadır. Bunlar; güvenlik açığını ilk fark eden kişi, kişiler ya da kurumlardır. Motivasyon kaynakları; bilgisayarları daha güvenli kılmak, teknik becerilerini piyasada göstererek kişisel reklamlarını yapmak ve şöhret kazanmak, üreticiyi önlem almaya zorlamak, merak, kafa tutma, maddi menfaat ve politik amaçlar olarak sıralanmaktadır [16].

Bu konuda 2000 yılından önceki dönemde ana motivasyon kaynağı genellikle şöhret iken son zamanlarda maddi teşviklerin daha önemli bir harekete geçirici olduğu görülmektedir. Diğer taraftan, güvenlik açığı avcılarının tek motivasyonu her zaman finansal olmayabilir. Maddi kazançla birlikte aynı zamanda piyasa tarafından bilinmek de son dönem teşvik programlarında öne çıkmaktadır [15].

Güvenlik açığı avcılığı; ayırt edici bir yetenek, bilgi ve birikim gerektirir. Ancak bu durum zamanla değişebilir. Konuya ilişkin yapılan çalışmalar, bu gruptaki insanların üçer yıllık döngülerle farklı şekillerde değişikliğe uğradıklarını göstermektedir. Yetenek, motivasyon, teşvik, etik duruş, sektör ve sektörler arası geçiş boyutları sürekli evrilmektedir [8].

Konu hakkında bir diğer çarpıcı husus ise, 0-gün (sıfır-gün) açığı bulma veya satma yönündeki eylemleri bir arada yapabilme kapasitesinin son derece sınırlı olduğu ve ancak birkaç binlerle ifade edildiğidir. 0-gün açığı bulanların üçte ikisinin, sonrasında yeni bir açığı tekrar bulamadıkları belirtilmektedir. Sistemler değiştikçe ve savunma güçlendikçe, zamanında çok verimli olan 0-gün açığı avcıları, faydasız ve işe yaramaz duruma düşebilmektedirler [8].

Güvenlik Bilgi Kaynakları[5]: Açığı Duyuranlar, Haber Kaynakları
Güvenlik haber kaynakları, mevcut açıklar hakkında; duyuru, ikaz, tavsiye bülteni vb. yayımlamak suretiyle kamuoyunu ve paydaşları bilgilendiren organlardır. Üretici web sayfaları, devlet veya özel güvenlik portalları, e-posta listeleri, güvenlik konferansları, uzman blogları bu kapsamda ele alınmaktadır. Bunların yanı sıra Packetstorm, SecurityVulns, Metasploit, Exploit Database© gibi istismar arşivleri de güvenlik haber kaynaklarına örnek olarak verilebilir.

Güvenlik haber kaynaklarının gösterdikleri performans, en uygun bilgiyi, doğru ve tarafsız olarak aktarabilmeleri ile orantılıdır. Bu bilgi kaynakları bağımsız ve güvenilir oldukları ölçüde, açık bir toplumdaki özgür basın görevini yürütürler. Açıklar konusunda kamuoyunun aydınlanmasını sağlayan ve uyarı işlevini yerine getiren adeta birer nöbetçi gibi davranırlar [16].

Frei'e göre; güvenlik haber kaynakları genelde güvenilir ve tutarlıdırlar. Bunlar tarafından sağlanan bilgiler de (ABD özelinde) genellikle birbiriyle örtüşen ve birbirini destekleyen niteliktedir. Kullanım ihtiyacına göre her birinden ayrı ayrı yararlanılmasında da fayda görülebilmektedir. Bu konuda tek başına en iyi bir çözüm bulunmamaktadır [16].

Düzenleyici Otoriteler ve Düzenlemeler
Düzenleyici otorite ve kurumlar, güvenlik açığı ekosisteminde hemen her bir aktörün yer alabildiği ve söz sahibi olabildiği bir bölümdür. Daha çok devlet veya devlet destekli organizasyonlar tarafından yönlendirilmekteyse de, yazılım şirketleri ve üçüncü taraf güvenilir paydaşlar da düzenleyici kurumlar içerisinde rol almaktadırlar. Düzenleyici kurumlar bazen haber kaynağı olma ve güvenlik açığı duyurma görevlerini de eşzamanlı olarak yerine getirmektedirler.

- MITRE[6] : 1958 yılında kurulan ve milli kritik konularda ABD devlet kurumları ile ortak çalışan, kar amacı gütmeyen bir kuruluştur. Sistem mühendisliği ve ileri teknolojiler konusunda devlete uzmanlık desteği sunmaktadır. Devlet destekli AR-GE merkezlerini[7] işletir. Bu merkezlerden birisi de 2014 yılında kurulan ve NIST[8] tarafından desteklenen Ulusal Siber Güvenlik

[5] Security Information Providers.
[6] "The MITRE Corporation" şirketinin kısa ifadesidir. Kısaltma değildir.
[7] Federally Funded Research and Development Center, FFRDC.
[8] National Institute of Science and Technologies.

Ar-Ge Merkezi'dir. Siber güvenlik konusu, çekirdek yetenekleri arasında bulunmaktadır [17].

- CVE[9] Güvenlik Açıkları Ortak Sözlüğü : CVE'den önce standart bir güvenlik açığı verisi bulunmadığından her firmanın kendi veri tabanını kullandığı bilinmektedir. Bu kapsamda, güvenlik açıklarının üreticiden bağımsız olarak, sistematik bir biçimde yönetilmesi ve sonrasında istatistiksel çalışmalara olanak tanıması ihtiyacı ortaya çıkmıştır.

MITRE, bu boşluğu doldurmak ve piyasa standardını belirlemek için 19 büyük güvenlik organizasyonunun da dâhil edildiği bir çalışma başlatmıştır. Bu organizasyonlar daha sonra büyük oranda, CVE'nin editörler kurulunu da (board) oluşturmuşlardır. CVE listeleri ilk olarak 1999 yılında yayımlanmaya başlanmıştır [16].

CVE, kamuoyu tarafından bilinen güvenlik açık ve zafiyetlerine dair kullanımı ücretsiz bir referans sözlüktür. Örnek bir CVE Şekil 2'de gösterilmiştir. Duyurulan her bir güvenlik açığına, tekil (unique) bir numara atamak suretiyle, güvenlik açığı yönetiminde; takip, koordinasyon ve otomasyonu mümkün kılmaktadır. Bir yazılım kusurunun CVE numarası almayı hak edecek gerçek bir güvenlik açığı olduğunun onaylanması bir dizi inceleme ve onay sürecine tabidir.

Şekil 2: Güvenlik Açığı CVE Bilgi Formatı, NVD (Örnek) [16].

Açıkları numaralandırma ve onaylama konusunda yetkili makam CVE Numaralandırma Otoritesidir (CNA[10]). Bu otoritenin üyeleri, MITRE, 22 adet yazılım şirketi ve üçüncü taraf (CERT/CC, ICS-CERT[11], JPCERT/CC[12]) güvenilir düzenleyicilerdir [18]. CVE, 1999 yılından bugüne kadar, akademi, devlet kurumları ve iş dünyasında fiilen geçerli bir uluslararası standart olarak kabul görmüştür.

- CWE: Ortak Yazılım Zayıflıkları Kataloğu: CVE listesinin 1999 yılında yayımlanmasından sonra, yazılımlardaki açıkların ve zayıflıkların tasnif edilmesi konusunda MITRE koordinesinde çalışılmalar başlatılmıştır. 2005 yılında, DHS[13] ve NIST[14]'in de dâhil olduğu SAMATE[15] projesi kapsamında 1500 güvenlik açığı, özelliklerine göre 290 başlık altında sınıflandırılmıştır.

Sistem mimarisi, tasarım veya kodlama boyutlarında tespit edilen ve her biri istismar edilmesi olası birer güvenlik açığına dönüşebilecek zayıflıklara yer verilen Ortak Yazılım Zayıflıkları Kataloğunda (CWE[16]) [19], 2011 Haziran itibariyle 860 tür hata bilgisi bulunmaktayken [20], 07 Aralık 2015 tarihinde yayımlanan son sürümünde (2.9) 1003 adet zayıflık türü tanımlanmıştır [19].

- NIST: Ulusal Standartlar ve Teknoloji Enstitüsü: NIST, 1901 yılından itibaren teknoloji alanındaki standartları belirleyen ve ABD Ticaret Bakanlığı'na bağlı olarak çalışan bir devlet kurumudur. Görevi kapsamında endüstriyel standartlar bulunmamaktadır. NIST araştırma laboratuvarlarında, kadrolu bilim insanları ile kapsamlı programlar yürütülmektedir [21].

Yönetilmekte olan ana programlardan birisi siber güvenlik konusudur. Kriptografi başta olmak üzere bilgi ve siber güvenliğe dair standartların oluşturulması öncelikleri arasındadır. Güvenlik Açıkları (ABD) Ulusal Veri Tabanı'nın (National Vulnerability Database, NVD) oluşturulması, işletilmesi ve idamesi NIST koordinatörlüğünde yürütülmektedir [22].

- NVD: Güvenlik Açıkları Ulusal Veri Tabanı: NVD, NIST bünyesindeki Siber Güvenlik Birimi'nin sorumluluğunda 1999 yılından itibaren oluşturulan bir veri tabanıdır. Güvenlik açığı verileri, burada otomatik yönetime uygun formatlarda yayımlanmaktadır [22].

CVE veri tabanı içeriğine NVD web sayfasından ulaşılabilmektedir. 2016 Mayıs ayı itibariyle yaklaşık 76.500 güvenlik açığı verisi tanımlanmış ve bu sayfadan duyurulmuştur. Herhangi bir açık ile ilgili olarak asgari; açığın ciddiyeti *(severity),* etki durumu *(impact)* ve derecesi *(rating)*, üretici *(vendor)*, yazılım ismi *(name)*, sürüm numarası *(edition)* ve açığın türü *(type)* bilgilerine yer verilmektedir. Bu veriler, saat başı güncellenmektedir [16].

[9] Common Vulnerabilities and Exposures.
[10] CVE Numbering Authority
[11] (ABD) Endüstriyel Kontrol Sistemleri SOME
[12] Japonya SOME Koordinasyon Merkezi

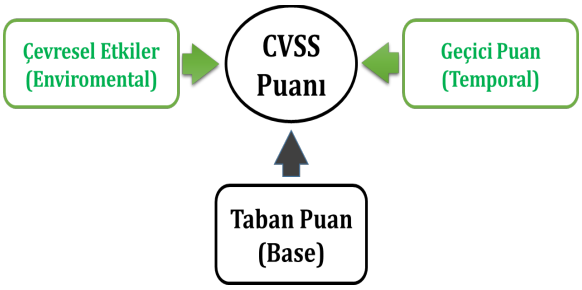
[13] U.S. Department of Homeland Security: *ABD İç Güvenlik Bakanlığı.*
[14] National Institute of Standarts and Technology
[15] Software Assurance Metrics and Tool Evaluation
[16] Common Weakness Enumeration.

NVD'de 19 adet açık türü kullanılmaktadır. En yaygın olarak duyurulan güvenlik açığı veri türü (CWE Type) kategorisinin, "Input Validation Error" ve "Design and Configuration Error" olduğu belirtilmektedir. NVD'de açığın ciddiyet düzeyi üç seviyeli olarak kullanılmaktadır. On üzerinden verilen puana göre bu seviyeler; Düşük (0-4), Orta (5-7), Yüksek (8-10) olarak belirlenmiştir.

- FIRST[17]: Siber Olaylara Müdahale ve Güvenlik Ekipleri Forumu: Değişik ülke ve kurumlardan SOME'lerin buluştuğu, 1990 yılında kurulan ve yaklaşık 350 üyesi bulunan bir platformdur. Güvenlik açıklarına ilişkin belirli hesaplamalar, otomasyon standartları ve formatları bu kuruluş tarafından geliştirilmiştir. Çalışmalarından en önde geleni CVSS[18] düzenlemesidir.

- CVSS: Güvenlik Açığı Puanlama Sistemi: CERT/CC, CISCO, MITRE, DHS, eBay, IBM Internet Security Systems, Microsoft ve Qualys gibi grupları kapsayan ve hâlihazırda FIRST tarafından koordine edilen müşterek bir girişimdir.

Açıkların ciddiyeti, Temel (*Base*), Geçici (*Temporal*) ve Çevresel (*Enviromental*) olmak üzere Şekil 3'de gösterildiği üzere üç boyutta değerlendirilir ve puanlanır [16]. Sıklıkla başvurulan ve dikkate alınan boyutun "Temel Puanlama" olduğu bilinmektedir.



Şekil 3: Güvenlik Açığı Ciddiyet Puanlaması [23].

CVSS'de, güvenlik açığı hakkındaki bilgilere standart bir formatta yer verilirken, yaratabileceği zafiyetin ciddiyetine ilişkin puanlama esasları da öngörülmektedir. CVSS'nin, 1.2.1. ve 2.0 (2007) sürümlerinden sonra 2015 yılı Haziran ayı itibariyle üçüncü sürümü (3.0) yayımlanmıştır [23].

- CERT, CERT/CC: 1988 yılında Morris Kurtçuğu'nun yayılması sonucu uğranılan zararlar nedeniyle, ABD Savunma Bakanlığına bağlı DARPA tarafından Carnegie Mellon Üniversitesi Yazılım Mühendisliği Bölümünde devlet destekli bir Ar-Ge Merkezi olarak kurulmuştur. Dört temel görevi; eğitim, koordinasyon, güvenlik açığı yönetim araçları geliştirme ve bu kapsamda bir bilgi deposu oluşturma olarak sıralanmaktadır.

Kullanıcılar tarafından tespit edilen güvenlik açıklarının, öncelikle üreticilere ve diğer teşvik programlarına iletilmesi tavsiye edilmekle birlikte, sıkı şartlar öne sürülmek kaydıyla güvenlik açıkları, bu platformlara ilave olarak CERT'e de raporlanabilmektedir. Sıklıkla karıştırıldığı diğer bir kurum olan US-CERT ile görev alanları birbirinden farklıdır [24].

- US-CERT: ABD İç Güvenlik Bakanlığına bağlıdır. Bünyesindeki Ulusal Siber Güvenlik ve Haberleşme Entegrasyon Merkezinde (NCCIC)[19] haftanın yedi günü 24 saat bilgisayar olaylarına müdahale edilmektedir. Bunun dışında Güvenlik Açığı Bilgilendirme Notları[20] yayımlamak suretiyle kamuoyunu bilgilendirmekte ve farkındalık yaratmaktadır. Siber güvenlik olayları US-CERT'e bildirilmekte, yazılım güvenlik açıklarını raporlamak isteyenler ise CERT'e yönlendirilmektedir [25].

US-CERT (DHS) tarafından yayımlanan Güvenlik Açığı Notlarında; teknik açıklamalar, etki (*impact*) durumu, kalıcı çözüm (*solution*) ve geçici çözüm (*workarounds*) önerileri ile bertaraf (*bypass*) yöntemleri ve etkilenen markaların isimleri (*vendor*) yer almaktadır. Daha ciddi güvenlik açıkları ise Teknik Alarmlar (*Technical Alerts*) ile duyurulmaktadır [16].

Güvenlik Açığı Pazarları

Yazılım güvenlik açıklarının işlenmesi ve duyurulması maksadıyla değişik piyasa ve platformlar oluşmuştur [11]. Güvenlik açıklarının, ücreti karşılığında el değiştirdiği bu piyasalar genel olarak; yasal pazar (*white market*), karaborsa (*black market*) ve gri pazar (*grey market*) olarak üç grupta tasnif edilmektedir.

- Yasal Pazar; Google, Facebook, Microsoft, Mozilla gibi üreticilerin güvenlik açığı bulma teşvik programlarının (*bug bounty*) yanı sıra, Bug Crowd, Hacker One's Internet Bugbounty, Pwn20wn, iDefense (2003), Zero Day lnitiative (ZDl)(2005) gibi diğer organizasyonlar yer almaktadır [16,8].

Açığı bulan kişi, güvenlik açığını, bu ortamlardan uygun gördüğü bir tanesine bildirmekte, önceden standart olarak belirlenmiş veya o güvenlik açığına özel olarak kıymet biçilmiş bir miktarı ödül olarak almaktadır.

[17] Forum of Incident Response and Security Teams.
[18] Common Vulnerability Scoring System.
[19] National Cybersecurity and Communications Integration Center.
[20] Vulnerability Notes.

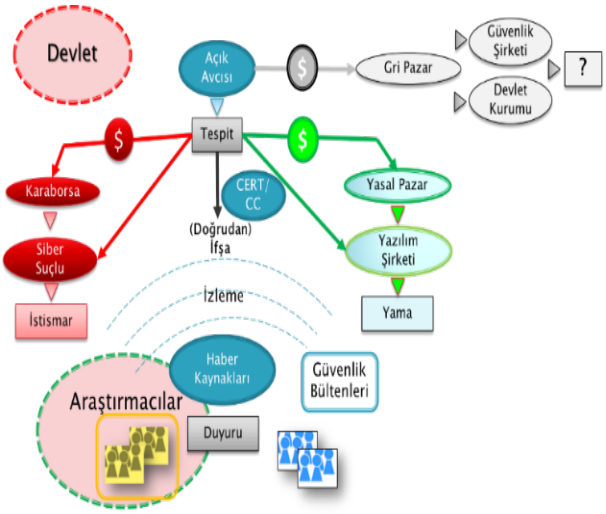
Yasal pazarın alıcıları, eğer o yazılımın üreticisi değillerse, ele geçirdikleri güvenlik açığını değişik şekillerde değerlendirmektedirler. Bu açığı, diğer güvenlik yazılım şirketlerine (müşterilerini ikaz etmede ön almaları için) veya o yazılımın geliştiricisine (yama üretmesi için) satmakta veya iletmektedirler. Bu senaryoda bazen, güvenlik yazılım şirketi, öncelikle kendi müşterilerinin etkilenmemesi için güvenlik açığını satın alıp, sonrasında yama geliştirmesi için üreticiye baskı yapabilmektedir [16].

Yasal pazar ifadesi ile alıcıların ve satıcıların hiçbir kötü niyet içerisinde olmadıkları düşüncesi, algısı ve varsayımı bir yanılgıdır. Bu pazarda kamu kurumları ve hatta bazı özel şirketler, açıklardan yararlanmak veya onları daha kazançlı müşterilere satmak için tedarik etmektedirler [16]. Buna örnek olarak, geçtiğimiz günlerde "ava giderken avlandığı" şeklinde haberlere konu olan İtalyan siber güvenlik şirketi Hacking Team verilebilir [26]. Müşterileri arasında 35 ülkeden yaklaşık 50 devlet kurumu da bulunan söz konusu firma, satmış olduğu servisler için kullandığı güvenlik açıklarını bu piyasalardan temin etmektedir.

Gri Pazar: Alıcılar arasında bu tür özel girişimlerin yanında devlet kurumlarının da görülmeye başlaması ile birlikte, gri pazar kavramı devreye girmektedir. Gri pazar yasaldır. Bu pazarın, başta ABD devleti, ona hizmet veren yüklenici firmalar ve istihbarat birimleri olmak üzere devlet organlarınca yönetildiği ve kullanıldığı algısı yaygındır [8]. Son dönemde konuya çarpıcı bir örnek olarak, San Bernardino/ABD saldırısı failinden ele geçirilen akıllı telefona erişim sağlanabilmesi için gösterilen gayretler verilebilir. Söz konusu telefonun "kırılabilmesi" için Apple Şirketi'nin işbirliğini reddetmesi sonrasında FBI[21], işlem yapabilmek maksadıyla gerekli güvenlik açığını bu pazardan temin ettiğini açıklamış, ancak açığın detaylarını ve işbirlikçisini kamuoyu ile paylaşmayacağını duyurmuştur [26].

Karaborsa: Güvenlik açıklarının alınıp satıldığı diğer bir ortam karaborsadır. Bu pazarı benzerlerinden ayıran husus, güvenlik açığının suç işlemek kastıyla, Yeraltı İnterneti (Deep Web, Dark Web vb.) üzerinden alınması ve buradaki alışverişin yasadışı olmasıdır. Siber suçlular, güvenlik açıklarını ya kendileri tespit etmekte, ya da karaborsadan tedarik etmektedirler. Bütün bu pazarları ve sürecin akış şeması Şekil 4'de gösterilmiştir.

Güvenlik açıkları, yazılım sahibi firma haricindeki aktörler tarafından satın alındığında, konunun yasal ve ahlaki boyutu üzerine tartışmalar doğal olarak artmaktadır. Açığı satın alan, bunu kamuoyuna duyurmadığı için, gerekli yama da üretilemediğinden güvenlik problemi devam etmektedir [15]. Özellikle kritik altyapılardaki (oy verme sistemleri, enerji tesisleri, finans, sağlık vb.) yazılımlara dair güvenlik açıklarının bu pazarlarda alınıp satılması, serbest piyasa ekonomisi ile açıklanması çok mümkün olmayan örneklerdir.



Şekil 4: Güvenlik Açığı Ekosistemi [16].

Fiyatlandırma ve Diğer Tartışmalar: Yazılım güvenlik açıklarının özelliklerini belirlemek ve değer biçmek son derece zordur [11,15]. Tespit edilen güvenlik açıklığının fiyatını belirleyen başlıca unsurlar: açığın bilinirliği ve yaygınlığı (yaygınsa değersizdir), güvenliğe etkisi, (ne kadar yüksekse o kadar kıymetlidir) ve ürünün popülerliği olarak sıralanmaktadır [16].

Bu kapsamda en muteber "ürün" grubu 0-gün açıklarıdır. Son derece ender bulunan ve geliştiricisi dâhil hiç kimse tarafından bilinmeyen bu tür güvenlik açıklarının karaborsada 50.000 ilâ 500.000 dolar arasında alıcı bulduğu rapor edilmektedir [3]. Microsoft, "bypass mitigation techniques" kapsamındaki açıkları bulanlara 100.000 dolar tutarında ödül vadetmektedir [8].

Güvenlik açığının değeri, ne yaptığıyla ve ne işe yaradığıyla doğrudan ilgilidir. Mobil cihazlardan daha ziyade masaüstü bilgisayarlarda kullanılan yazılımlardaki açıklar daha değerli olmakta, uzaktan kod çalıştırmayı etkinleştirebilmesi, açığa ilave değer katmaktadır [8].

1995 yılında Netscape tarafından başlatılan ilk teşvik programından bu yana oldukça mesafe kat edilmiştir. Başta Google, Facebook, Microsoft gibi büyük firmalar

[21] Federal Bureau of Investigation.

olmak üzere, yazılım geliştiren firmaların, ürünlerindeki güvenlik açıklarını bulmaları için insanları harekete geçirme girişimleri sektörde yaygın bir tercih haline gelmiştir [27].

Örneklendirmek gerekirse; Microsoft teşvik programının başladığı 2013 yılı Haziran ayından [28] Temmuz 2014'e kadar geçen yaklaşık bir yıllık sürede sadece yedi ayrı araştırmacıya toplamda 253.000 dolar ödenmiştir [11]. 2000-2007 arasındaki toplam yazılım açıkların yaklaşık %10'unun, HP ZDI ve iDefense programları sayesinde bulunduğu belirtilmektedir [29]. Bu tip programlar yoğun ilgi çekmiştir. 2011 yılında başlatılan Facebook teşvik programına bugüne kadar dünya genelinden 2400 geçerli rapor iletildiği, 800'den fazla araştırmacıya 4,3 milyon dolar ödendiği [30], açığı bulan kişilerin yaşının ise 10'a kadar düştüğü belirtilmiştir [31]. Diğer taraftan, teşvik programlarında başarı gösterenler, daha sonra bu şirketler tarafından tam zamanlı çalışan olarak işe alınabilmektedir [15,32].

Yukarıda verilen bilgiler ışığında, teşvik programları kapsamında özetle Güvenlik Açığı Ödül Programları[22] ve 0-Gün Açığı Pazarları[23] olmak üzere iki akımdan bahsedilebilir [15].

Açığa dair bilginin ne şekilde olursa olsun el değiştirmesi tartışmalı bir konudur. Çift kullanımlı (dual-use) askerî teknolojilerin yayılımını kısıtlayan 1996 tarihli Wassenaar anlaşması hükümlerini bu alana uyarlayan yaklaşımlar mevcuttur. Diğer taraftan açığın bir ticari sır olup olmadığı, ülke dışına satılmasının bu anlamdaki etkileri, maden, doğal kaynaklar veya hazine gibi aslında keşfedilmeyi bekleyen bir meta gibi mi değerlendirilmesi gerektiği tartışmaları uzayıp gitmektedir [16].

Teşvik programlarına ilişkin artan tartışmalara bakıldığında; teknolojik, ekonomik, kurumsal ve yasal bir takım değişiklik ve düzenlemelere ihtiyaç bulunduğu açıkça görülmektedir [11]. Buna paralel olarak teşvikler sayesinde güvenlik açığı bulma oranlarının çarpıcı bir biçimde yükseldiği değerlendirmeleri de yaygındır [33].

Müşteriler: Yazılım şirketlerinin kendi ürünlerine dair güvenlik açıklarına erişmek maksadıyla yürütmüş oldukları faaliyetlere yukarıda değinilmiştir. Bu faaliyetlere, ücreti karşılığında açığın edinilmesi de şüphesiz eklenebilir. Konunun bu kısmı yukarıda ayrıntılı olarak işlendiğinden, müşteriler başlığı altında daha çok; güvenlik şirketleri, devlet ve siber suçlulara ilişkin hususlara yer verilmiştir.

Siber Güvenlik Şirketleri: Ticari hayatları yararına görünürlük kazanma, haber değeri taşıyan güvenlik açıklarına hükmetme yoluyla imaj ve itibarlarını artırma, ürettikleri güvenlik sistemleri (IDS, IPS vb.) için ilave koruma sağlayarak müşterilerine avantaj sağlama ve paralı bir hizmet olarak bunu sunarak gelirlerini artırma maksadıyla güvenlik açığı bilgilerine sahip olmak istemektedirler [16].

VUPEN, Endgame, Netragard, ZDI gibi güvenlik firmaları; tedarikçileri ve müşterileri güvenlik açığı alım/satım pazarlarında bir araya getirmişlerdir [11]. Bu anlamda, piyasadaki ana aktörlerin bugün için iDefense ve ZDI olduğu söylenebilir. Bunların yanında Qualys gibi güvenlik şirketlerinin topladığı büyük hacimli veriler de ilgili firmalardaki gerçek sistemlerden elde edildiklerinden önem ve değer taşır [16].

Security Tracker, Security Works, Metasploit Project Symantec DeepSight, FireEye, Logrhythm, Cyveillance, RSA Live, Dell SecureWorks, IlD ActiveTrust, ThreatCloud, lntelliStore, Security Focus gibi girişimler de sektöre "tehdit ve zafiyet istihbaratı" sağlayan diğer önemli çabalar olarak sıralanmaktadır.

Bu kapsamda CVE veri tabanında en çok referans gösterilen bilgi kaynaklarının; Secunia, Security Focus, IBM ISS X-Force, Bugtraq, FrSIRT, OSVDB, Security Tracker ve CERT olduğu belirtilmektedir [16].

Güvenlik şirketlerince açıklara ödenen ücret çoğu zaman açıklanmamakla birlikte, ZDl tarafından "baş araştırmacılarına" ortalama 20.000 dolara kadar ödeme yapıldığı, güvenlik açıkları alanında çalışan yaklaşık 6000 kişiden %40'ının ZDI'nın araştırmacıları olduğu rapor edilmektedir. Yapılan araştırmalarda, bunlardan büyük bölümünün iş taahhüt ve bağlantılarına sadık olduğu ve sadece %10'unun karaborsada daha yüksek ücret teklif edildiği takdirde bulduğu açığı 'potansiyel' suçlulara satabileceğini ifade ettiği belirtilmiştir [16].

ABD menşeli örneklerin yanı sıra, 2002'de Danimarka'da kurulmuş olan Secunia (2015'de Flaxera tarafından alınmıştır), 2003'de kurulan Fransız menşeli FrSIRT (2008'de adı VUPEN olarak değişmiştir) ve 1997'den itibaren sektörde görülen Rus Kaspersky Lab.[34] diğer önemli güvenlik şirketlerinden sayılabilir.

Siber Suçlular: Ticari casusluk, finansal dolandırıcılık ve siber zorbalık gibi yöntemlerle güvenlik açıklarını çoğunlukla maddi getiriye dönüştürme maksatlı hareket eden siber suçlular devlete göre her zaman daha esnektirler ve değişikliklere çabuk adapte olabilmektedirler. Siber suçlular, güvenlik açığı duyuruları ve güvenlik bültenlerini takip ederek ve

[22] Vulnerability Reward Programs.
[23] Zero Day Markets.

yamaları inceleyerek yaptıkları tersine mühendislik yoluyla yeteneklerini geliştirirler [16]. Hedeflerine ulaşabilmeleri, kendilerini sürekli güncel tutabilmelerine ve güvenlik açıklarına duydukları ilgiye bağlıdır.

Siber suçların, 2016 yılı için küresel ekonomiye 445 milyar dolarlık bir zarar oluşturacağı tahmin edilmektedir. "Hackerlar", bu alanda her geçen gün daha da gelişmekte ve organize hale gelmektedirler. Güvenlik açıklarını bulmak görece kolaylaşmakta, buna bağlı olarak suçluların çalışma modelleri sürekli değişmektedir. Araştırmalar, bir siber suçlunun saldırı yaparken kullandığı araçların ortalama 1.500 dolar tuttuğunu göstermektedir. Bunun yanında, bir siber suçlunun yaklaşık olarak yıllık 30.000 dolar kazandığı belirtilmekte, bu ücret ise, ABD'deki üst düzey bir siber güvenlik uzmanın maaşının yaklaşık dörtte birine tekabül etmektedir [35].

Devlet: Yazılım güvenlik açıkları piyasasındaki etkin aktörlerden bir diğeri devlet kurumları ve bunlara hizmet verenler olarak görülmektedir. Piyasayı düzenleme, kamuoyunu bilgilendirme ve gerektiğinde açıklardan istifade etme yönüyle devlet kurumlarından bir bölümünün güvenlik açıklarına karşı ilgili olduğu anlaşılmaktadır. Bu ilginin birçok sebebi varsa da, en önemlilerinden biri, devletlerin bu açıkları bir kuvvet çarpanı yetenek olarak kullanmak suretiyle siyasi, ekonomik ve askerî avantajı kazanma niyetleri olarak ifade edilebilir.

Benzer şekilde, ABD Devleti ve istihbarat kurumları tarafından da bu pazarın doğal bir düzenleyicisi ve parçası olarak, açıkları satın almak ve bu açıkları istismar edebilecek araçlar geliştirmek için milyonlarca dolarlık bütçe kullandığı ifade edilmektedir. Bu maksatla ABD Ulusal Güvenlik Kurumunun (NSA[24]) 2013 yılında yaklaşık 25 milyon dolarlık harcama yaptığı belirtilmektedir [11].

Akademik Çevre: Güvenlik açığı ekosistemine dair nicel çalışmalar, henüz "emekleme" aşamasındadır [16]. Bugüne kadar bu konuların akademik camiada çok fazla tartışıldığı söylenemez [15]. Diğer taraftan konuya karşı giderek artan bir ilgi ve buna paralel olarak bilimsel çalışma sayısında yükseliş görülmektedir.

Bu kapsamdaki öncü çalışmalar içerisinde; Rescorla'nın 2003-2004 yılında yaptığı ve yazılım açıklarının bulunmasına yönelik gayretleri sorguladığı çalışma ile 2004 yılında Ozment ve Schester'in, teşvik programlarının faydalarını inceledikleri araştırmalar sayılabilir [15].

[24] National Security Agency.

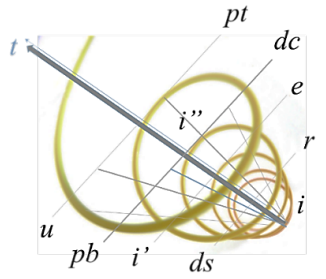
Konuya ilişkin olarak; Frei (2009) [16], Carr (2010) [36], Bilge (2012) [29], Egelman (2013) [15] ve Holm (2015) [37]'ün araştırmaları, ekosistemi anlaşılır kılmaya dönük öne çıkan nitelikli çalışmalar arasındadır. Paydaşları aydınlatma yönündeki araştırmaların artmasıyla, ekosistem içerisinde, akademik çevreler de yerini almaya başlamıştır.

2.2. Güvenlik Açığı Yaşam Döngüsü: Süreçler, Yöntem ve Araçlar

Bir güvenlik açığının yaratılmasından, geçerliliğini yitirdiği güne kadar geçen sürenin, bir yaşam döngüsü içerisinde tanımlanması ve safhalandırılması zordur. Yazılım geliştirmenin hangi aşamasında ve ne şekilde açığın oluştuğu, kusur olarak bile tanımlanamayacak bir hatanın, yazılım derlendikten sonra veya başka bir işlevin yazılıma eklenmesiyle açığa dönüşüp dönüşmediği tam olarak bilinememektedir.

Güvenlik açığı avcısının, yazılımdaki problemi ne zaman tespit ettiği, tespit için ne kadar gayret sarf ettiği veya bu bilginin kamuoyuna duyurulmasına kadar ne kadar süre geçtiği hiçbir zaman net olarak bilinememekte, bilindiği durumlarda ise çoğunlukla paydaşların beyanı esas alınmaktadır.

Dolayısıyla bütün bu olayların bir zaman çizelgesi üzerinde birebir karşılığını aramak doğru değildir. Süreç, doğrusal olmaktan daha çok döngüsel niteliktedir. Faaliyetler bazen sırasıyla, bazen eş zamanlı olarak, kimi zaman ise belirli safhalar atlanarak veya bazı adımlar hiç yaşanmayarak ilerlemektedir.



Şekil 5: Süreçler: Güvenlik Açığı Yaşam Döngüsü[25]

Şekil 5'de değişik bir yorumla sunulan Ozment'in tasnifi ile bu döngü içerisindeki kilometre taşları, bir zaman (***t***-time) çizelgesi üzerinde; açığın doğum tarihi (***i***-injection), yazılımın piyasaya sürülme tarihi (***r,*** release), açığın tespit edilme tarihi (***ds***-discovery), istismar kodunun hazır olma tarihi (***e***-exploit/scripting), açığın ifşa tarihi (***dc***-disclosure[26]), açığın kamuoyuna

[25] Şeklin spiral bölümü, www.istockphoto.com adresinden alınmıştır.

[26] Açığı keşfedenin, yazılım geliştiriciyi ya da ilgili kurumu açığa ilişkin haberdar ettiği tarihtir.

duyuru tarihi (***pb***-public), yama yayımlama tarihi (***pt***-patch) ve yama uygulama tarihi (***u***-update) şeklinde sıralanmıştır [38].

OSVDB[27] ve NVD'nin tanımlarına göre; ifşa tarihi, güvenlik açığı hakkında kamuoyunun haberdar edildiği tarih, duyuru tarihi ise açığın veri tabanında yayımlandığı tarih olarak açıklanmıştır [20]. Duyuru tercihine göre aslında her iki tarih de teknik olarak aynı anlama gelmektedir.

Aşağıda bu safhalardan sürece ilişkin görece önemli olduğu değerlendirilen; tespit, duyuru, yama ve istismar adımlarına yer verilmiştir.

Açığı Tespit Etme

Yazılımlardaki açığı tespit etmek, koda farklı bir gözle ve değişik bir açıdan bakmayı gerektirir [8]. Yazılımdaki bir kusur; bizzat yazılımcısı tarafından henüz geliştirme aşamasındayken, şirketin yazılım uzmanlarınca test aşamasındayken, deneme sürümü sırasında gönüllü deneyiciler tarafından veya piyasaya sürüldükten sonra uç kullanıcılarca tespit edilebilir.

Ockhavi ve Nizol'a (2008) göre güvenlik yamalarından bazıları, yeni açıklara neden olabilmektedir [8]. Yazılımda bulunan her bir açıktan sonra geride daha az açık kalıp kalmadığı da araştırılan konulardandır [15].

Bir yazılımdaki açıkların bulunma oranını artıran başlıca faktörler; yazılımın kod büyüklüğü, kullanıma sunulduğundan itibaren geçen zaman (yazılımın yaşı), yazılımın bilinirliği ve yaygınlığı ile olgunluk düzeyi olarak sıralanmaktadır [20,8]. Bu nedenle araştırmacılar 2012-2013 yıllarından itibaren, çok daha popüler olan ve yaygın kullanılan web tarayıcılara (Internet Explorer, Mozilla, Chrome vb.) ve istemci tarafındaki ürünlere yoğunlaşmışlardır [8].

2002-2007 yılları arasını kapsayan bir araştırmada, herhangi bir günde yama üretilmemiş açık sayısının Microsoft için 0 ilâ 22 (Ortalama 11,4) Apple için ise 0 ilâ 55 (Ortalama 24,7) arasında olduğu tespit edilmiştir [16]. Hâlihazırda kullanılan yazılımların kapsamı ve karmaşıklığı göz önüne alındığında sayıların bugün için çok daha büyük olması beklenebilir. İçinde bulunulan böylesi bir ortamın siber suçlular için son derece verimli olduğu açıktır.

Güvenlik açıklarının tespit zamanları kapsamında yıl içerisindeki dönemlere bakıldığında ise, yama üretimi anlamında bir temizleme gayreti olarak görülebilecek yılsonu yoğunluğu belli belirsiz göze çarpmaktadır. Buna ilave olarak her yıl Temmuz ve Ağustos aylarında icra edilen Defcon ve Blackhat gibi konferanslarda güvenlik açığı avcılarının kendilerini göstermek adına faaliyetlerin öncesi ve sonrasında açık bulma çabalarını artırmaları nedeniyle de özellikle Microsoft ürünlerinde bu dönem için bir yoğunluktan bahsedilmektedir [20].

Açığın ne zaman tespit edildiği, tespit edenin motivasyonuna bağlı olarak çoğunlukla hiçbir zaman bilinememekte ve rapor edilmemektedir. Buna rağmen, tespit zamanı bilgisinin alınabileceği bazı kaynaklar mevcuttur. Bu kaynaklara bir örnek olarak, 5 Nisan 2016 itibariyle faaliyetlerini sonlandırdığını duyuran OSVDB verilebilir [39]. Güvenlik açıklarının el değiştirdiği diğer bazı platformlarda da bu bilgiye zaman zaman yer verilmektedir [16].

Yazılım güvenlik açıklarının genelde parasal bir değeri vardır. Bulunan bir açık için kimi durumda, karaborsa veya gri pazarda, yasal pazarda verilen ücretin 120 katına kadar fazla bir ücret önerilebildiği görülmüştür [8]. Bu pazarlarda açığı satın alanlar, bunun yanında güvenlik açığının istismar edilebilir olduğunun garantisini de talep etmektedirler [8].

Diğer taraftan, güvenlik açıklarının maddi değeri arttıkça, bu açığın bizzat yazılımcısı tarafından, daha sonra kendisince "bulunmak" üzere yazılıma yerleştirilmesi ihtimali (kobra etkisi[28]) de tartışılmaktadır [15].

Ayrıca, açığı tespit eden kişinin, bu bilgisini, karaborsada sattıktan sonra, yazılım üreticisi veya yetkili diğer kurumlarla da paylaşması durumunda (veya tersi durumda) ne tür tedbirler alınabileceği, hatta tedbir alınıp alınamayacağı konusu da değerlendirilmelidir. Mevcut durumda bu konu, araştırmacının itibarını koruma güdüsü, kişisel güvenilirliği ve karşılıklı güven ile taahhütler üzerine kurgulanmıştır [16].

Güvenlik Açığını Duyurma

Güvenlik açığını tespit eden kişi, açık bilgisini; bu yazılımı geliştiren yazılım üreticisine, yazılımı kullananlara (devlet veya firmalara) ya da siber suçlulara verebilir. Bunların hiçbirini tercih etmeyerek güvenlik açık bilgisini doğrudan kamuoyuna da duyurabilir. Bazen de yazılımdaki güvenlik açığı bir siber saldırı sonrasında öğrenilebilir. Ne şekilde haberdar olunursa olunsun, açığın duyurulmasıyla saldırılar artmakta ve açığa dair yama yayınlansa bile yama yapmamış sistemler daima bulunmakta ve hedef alınmaktadır [8].

Güvenlik açığının nereye ve ne şekilde raporlanabileceği ve açık bulunan yazılıma dair hangi

[27] Open Source Vulnerability Database.

[28] Cobra Effect.

teşvik programları bulunduğu hakkında detaylı ve yeterli bilgiye rahatlıkla ulaşılabilecek çok sayıda kaynak mevcuttur [40,41,42,43,44]. ABD'de bu konuda ana koordinatör ve yetkili makam CERT/CC'dir [45].

CERT/CC'ye göre beş tür duyuru seçeneği bulunmaktadır. Bunlar; saklı tutma ve duyurmama, kısmen duyurma, tamamen ifşa etme[29], sorumlu davranış[30] ve koordineli duyurma[31] olarak sıralanmaktadır [45]. Açıkların duyurulması, etik ve yöntemsel boyutlarıyla tartışma konusudur [8]. Duyuru tercihinin, yamayı hazırlama ve yayınlama davranışını nasıl etkilediğine dair de çalışmalar yapılmıştır [16].

CERT/CC tarafından açığın giderilmesi için yazılım firmalarına verilen süre normalde 45 gündür. Çok ciddi sonuçları olabileceği değerlendirilen açıklar için bu süre uzatılabilmekte veya bazı durumlarda güvenlik açığı, kamuoyuna hiç duyurulmayabilmektedir [46].

Açıkların duyurulması tartışması dâhilinde**;** biri "Şeffaflık Sayesinde Güvenlik", diğeri ise "Gizlilik ile Güvenlik" olmak üzere iki temel yaklaşım bulunmaktadır. Bu yaklaşımlardan birincisinde, açığın hemen duyurulmasının etkili olacağı, zira güvenlik açığını öğrendikleri için kullanıcıların tedbir alacakları, üreticilerin ise daha güvenli yazılım geliştirme ve bir an önce yama çıkarma konusunda zorunluluklarının artacağı savunulmaktadır. İkinci yaklaşımda ise, açığın mümkün olduğunca duyurulmaması, çünkü saldırganların bu açığı kullanarak her şeyi alt üst edebilecekleri iddia edilmektedir. Zaman içerisinde üçüncü bir yaklaşım olarak "Sorumlu Davranış" seçeneği ortaya çıkmış ve büyük oranda benimsenmiştir [16].

Sorumlu Davranış seçeneği en makul hareket tarzı olarak görülmekle birlikte bu modelin işe yaraması için bazı boyutların iyi çalışması gerekmektedir. Bunlar; iyi kaleme alınmış, yayımlanmış ve paydaşlarca benimsenmiş süreçler, açıkları raporlayan ve kamuoyuna duyuranların dürüst ve tutarlı olmalarının yanında takip ve denetimleri, üretici tarafından duyuru ve yayınlarında açığı bulan kişinin bilgilerine de yer verilmesi olarak sıralanmaktadır [16].

Açık duyurusu yapmak güvenlik ekosistemi için önemli bir olaydır. Güvenlik bilgilerine zamanında ve kısıtsız erişim, açığın etkilerini en aza indirgemek için en iyi yoldur. 2000'li yılların başında açıkların %24'ü kamuoyuna duyurulmadan önce sektörün içindekiler tarafından bilinmekteyken, 2007 yılına gelindiğinde bu oran % 80' yükselmiştir [16].

İfade ve paylaşma özgürlüğü, ticaret mevzuatı, patent ve telif hakları, uluslararası taahhüt ve yaptırımlar, elektronik ortamla ilgili diğer düzenlemeler [47] gibi boyutları bulunan açıkları duyurma faaliyeti, bazen mahkemelerde sonuçlanan hukuki anlamda da tartışmalı bir konudur [16]. Bu nedenle, özellikle ABD'de, süreçler ve yöntemler olabildiğince detaylı tanımlanmıştır ve mekanizmalar ciddiyetle işletilmektedir. Security Focus'un Avrupa Birliği ülkelerinden avukatlarla yaptığı mülakat sonucunda, ABD'nin aksine çoğu Avrupa ülkesinde ise bu konuda yasal bir düzenlemenin olmadığı ortaya çıkmıştır [16].

Güvenlik açığı kamuoyuna duyurulmadan önce, bu konuda yetkili makam olan Numaralandırma Otoritesi (CNA[32]) tarafından, kendisine gelen başvuru incelenir ve ayrılmış (*reserved*), ihtilaflı (*disputed*) ve reddedilmiş (*rejected*) olarak etiketlenir [16].

CVE Editörler Kurulu'nun içerik ekibi tarafından başvurular analiz edilir, araştırılır ve işlem yapılır. Bu ekip, içeriğin tamamından sorumlu olan editöre bağlıdır. Güvenlik açıkları, Editörler Kurulu'ndan geçtikten sonra CVE listesine girer. Eğer bir başvuru reddedilirse, gerekçeleriyle birlikte duyurulur. Editörler Kurulu'nda; güvenlik organizasyonları, akademi temsilcileri, araştırma enstitüleri, devlet kurumları ve diğer önde gelen güvenlik uzmanları bulunur. Sürecin yönetimi MITRE tarafından yapılır. Hâlihazırda Editörler Kurulu'nun, 22 farklı organizasyondan 31 üyesi bulunmaktadır [16].

Bir güvenlik açığını hakkıyla tanımlayabilmek, gerçek durumunu ortaya koyabilmek ve derecelendirmek hassas ve zor bir konu olarak görülmektedir. Bu nedenle, yürütülen çalışmalarda CVE tanımlarına itibar edilmektedir.

Yama Yönetimi: Hazırlama, Duyurma, Güncelleme

Herhangi bir güvenlik açığı kendisine raporlandığında, yazılım üreticisi tarafından düzeltici tedbirin bir an önce alınması gerekmektedir. Bu önlem, açığı kapatacak bir yamanın geliştirilmesidir. Yamanın yayımlanması da tek başına yeterli değildir. Yamanın, açığın bulunduğu sistemlere uygulanarak sistemlerin güncellenmesi şarttır. Yama yönetimi, güvenlik açığı yönetiminin önemli bir aşamasını oluşturur.

Genelde açığın tespit edilmesinden itibaren ortalama 120 gün sonra güvenlik yaması yayımlanmaktadır. Tespit edilen bir açığın bir takvim yılı içerisinde bir

[29] **Full Disclosure:** Açığa dair her tür bilginin (kavramsal ispat [proof-of-concept] dâhil) kamuoyuna duyurulmasıdır.

[30] **Responsible Disclosure:** Açığı sorumlulara bildirerek, yama için makul bir süre tanıma.

[31] CERT/CC ve Microsoft'un, tercih ettiği bir kavramdır. Aslında sorumlu davranış ile aynı şeyi ifade etmektedir [45].

[32] Candidate Numbering Authority.

başkası tarafından bulunması ihtimalinin %10 olduğu belirtilmektedir [8].

Yapılan bir başka araştırma, Windows© işletim sistemi kullanılan bir bilgisayar için, güvenlik açıkları kamuoyuna duyurulduğu anda, ancak % 65'i için güvenlik yamasının hazır olduğunu göstermektedir. Secunia'nın araştırmasına göre ise Windows kullanıcıları yılda yaklaşık 300 adet güvenlik açığına maruz kalmaktadırlar [29].

Yama yönetiminde uç kullanıcıların davranışları ve özellikle kurumsal kullanıcıların yama yapma konusundaki titiz ve yavaştan alma tercihleri, açıkların daha uzun süre risk yaratmasına neden olmaktadır [16]. Sektöre göre değişmekle birlikte, ortalama bir yazılımın sayıca yarısına yama uygulamak için geçen süre *(half-life)* yaklaşık 30 gündür. Güvenlik açıklarının o yazılımdaki yaygınlık oranı *(Prevalence)* %50-60, duyurudan itibaren istismar süresi 10 günden az, devamlılığı *(Persistence)* ise teorik olarak sonsuz olarak açıklanmaktadır [20].

İstismar

Potansiyel bir siber suçlu, bir yazılıma dair açığı tespit ettiğinde veya bu açığı edindiğinde, ilk olarak, açığın işe yaradığını göstermek için bir istismar[33] kodu geliştirmektedir. İstismar kodu; bir parça yazılım, bir virüs, bir dizi veri veya sıralı komutlardır. İstismar yoluyla bir yazılımda veya gömülü bir sistemde beklenmedik ve istenmedik bir etki veya davranış yaratmak üzere güvenlik açığından yararlanılır. Güvenlik araştırma ve analiz araçlarının içerisinde bulunan kavramsal ispatlar[34] veya istismar gereçleri (exploit kit) de bu kapsamda değerlendirilir [16].

Güvenlik açıkları benzerlik gösterdiklerinde; *XSS*, *SQL Injection*, *Arbitrary Long Input Fields* gibi bilinen yaygın bir açık sınıfına dâhil edilirler [16]. İstismarların %94'ü, güvenlik açığı kamuoyuna duyurulduktan sonraki 30 gün içerisinde meydana gelmektedir [29].

Sıfırıncı Gün (0-gün) Açıkları

Güvenlik açığı ve istismar konusu çalışılırken 0-gün açıklarına değinmek bir zorunluluktur. 0-gün açığına karşı hemen hemen hiçbir savunma imkânı bulunmamaktadır. Antivirüs yazılımlarının veya saldırı tespit ve önleme sistemlerinin imza tabanlı tarama ile bu saldırıları fark etmeleri mümkün değildir [29].

Tipik bir 0-gün açığı, kimsenin haberi olmadan ortalama 300 gün boyunca etkisini sürdürmekte, bazı durumlarda bu süre 2,5 yıla kadar uzayabilmektedir. 0-gün açığının kamuoyuna duyurulması sonrasında saldırı miktarı ise yaklaşık 100.000 kat artmaktadır [29].

Symantec analistleri tarafından çoğu Windows© tabanlı, IE ile Adobe vb. yazılımlar olmak üzere 2006-2011 arasında (2008:9, 2009:12, 2010:14 (Stuxnet ve Hydraq etkisi), 2011:8) her yıl için ortalama 8 ilâ 15 arasında 0-gün açığı tanımlanmış, Qualys analistlerince ise 2009 yılı için 54 adet aynı tür güvenlik açığı rapor edilmiştir [29].

III. ABD HARİCİNDEKİ DİĞER BAZI ÜLKELER

Siber uzayın etkin ve aynı zamanda teknoloji öncüsü ülkelerinden seçilen belirli başlılarında güvenlik açığı konusunun ne şekilde ele alındığına dair bilgi ve değerlendirmeler özet şekilde aşağıda sunulmuştur. Müstakil ve özgün bir güvenlik açığı ihbar, işleme ve yönetim sistemi olsun veya olmasın bu ülkelere ilişkin bilgiler, ABD modeli kapsamında yukarıda anlatılan hususlar için de tamamlayıcı niteliktedir.

3.1. Japonya

Japonya'da güvenlik açıkları ciddi olarak ele alınmakta ve yönetilmektedir. Herhangi bir web sayfasında veya uygulama yazılımında tespit edilen güvenlik açığı Bilişim Destekleme ve Tanıtım Kurumuna (IPA[35]) rapor edilmektedir. IPA tarafından analiz edilen ve kıymetlendirilen güvenlik açığı, bu konuda yetkili ve koordinatör makam olan Japon Bilgisayar Olaylarına Müdahale Ekibi Koordinasyon Merkezi'ne (JP-CERT/CC[36]) iletilir. JP-CERT/CC, açığı, yazılım üreticisi ve FIRST ile koordine ederek muhtemel yama üretme tarihi ile kamuoyuna duyuru zamanını belirler.

Süreç, Şekil 6'da resmedilmiştir [50]. JP-CERT/CC'nin konuyla ilgili olarak etkin ve etkili bir kuruluş olduğu görülmektedir. CVE Numaralandırma Otoritesi'nde koordinatör ve FIRST yönetim kurulunun bir üyesi, aynı zamanda Asya Pasifik Bölgesi Müdahale Ekiplerinin (AP-CERT) de başkanıdır [49].

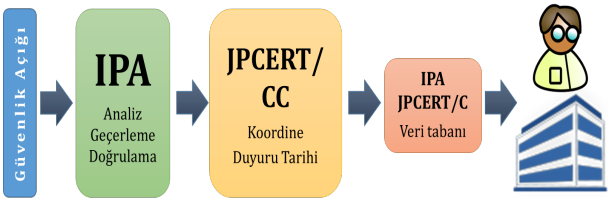
Bilgi Güvenliği Erken Uyarı ve İşbirliği[37] girişimi kapsamında devlet kurumları, sivil kurumlar ve akademik camia arasında organize ve sıkı bir işbirliği bulunmaktadır.

Konuyla ilgili başlıca aktörler; Elektronik ve Bilişim Sanayicileri Derneği (JEITA[38]), Bilgisayar Yazılımcıları Derneği (CSAJ[39]), Bilişim Hizmetleri Derneği (JISA[40])

[33] Exploit
[34] Proof-of-concept

[35] Information-Technology Promotion Agency(2002)
36 Japan Computer Emergency Response Team/Coordination Center (1996).
[37] Information Security Early Warning Partnership.
[38] Japan Electronics and Information Technology Industries Association.
[39] Computer Software Association of Japan.

ve Ağ Güvenliği Derneği (JNSA[41]) olarak sıralanmaktadır.



Şekil 6: Japonya Güvenlik Açığı Yönetim Sistemi [50].

Güvenlik açığı bilgileri IPA tarafından, önceki bölümlerde tanıtılan format ve usullere benzer şekilde; bilgilendirme bültenleri (JVN[42]) ve ikaz duyuruları (JVN iPedia[43]) şeklinde yayımlanmaktadır. Bu kapsamdaki bilgiler, güvenlik açığı bilgisini ülke içerisinde olduğu gibi dışında da duyurma yeteneğini ve uluslararası işbirliğini geliştirmek maksadıyla, İngilizce olarak da ayrıca yayımlanmaktadır.

3.2. Almanya

Siber güvenlik, yüksek öncelikli bir konu olarak, kapsamlı bir strateji (2011), oturmuş sorumluluklar ve yetkili kurumlarla ele alınmaktadır [51].

Siber güvenliğin çerçevesi yasal olarak güçlü bir biçimde çizilmiştir. Konuya ilişkin en yetkili makam Federal Bilgi Güvenliği Ofisi (BSI[44])'dir. BSI bünyesinde siber olaylara müdahaleden sorumlu CERT-BUND bulunmaktadır.

Bunun haricinde 28 adet CERT ile, büyük bir siber olaylara müdahale ağı kurulmuş ve işletilmektedir. Kamu, özel sektör ve akademi arasındaki işbirliği ve koordinasyon iyi seviyededir. BSI ve Afet Yönetim Başkanlığının (BBK[45]) birlikte yürüttüğü Kritik Altyapıların Korunması Programı (UP KRITIS) ile BSI bünyesindeki Siber Güvenlik İttifakı (AFC[46]) öne çıkan girişimlerdir.
CERT-BUND'un görevleri arasında; güvenlik açıklarına karşı uyarı ve bilgilendirme ile açıkların giderilmesi için uygulanabilir öneriler sunmak bulunmaktadır [52].

Yazılım güvenlik açıklarının ihbar, işlem ve raporlanmasına, kısacası yönetimine ilişkin doyurucu bilgi ile yaşayan mekanizma ve süreçlerin varlığı ise tespit edilememiştir.

[40] Japan Information Technology Services Industry Association.
[41] Japan Network Security Association
[42] Japan Vulnerability Notes.
[43] Vulnerability Countermeasure Information Database.
[44] Federal Office for Information Security.
[45] Federal Office of Civil Protection and Disaster Assistance.
[46] Allianz-Fuer-Cybersicherheit.

3.3. Hollanda

Siber güvenliğe yönelik olgun bir yasal ve siyasi altyapı bulunmakta, bu altyapının çerçevesi ikincisi 2013 yılında yayımlanan Güvenlik Stratejisi'ndeki kapsamlı ve açık hedeflerle çizilmektedir. Strateji belgesi, iki yılda bir güncellenmektedir [51].

Ulusal Siber Güvenlik Merkezi (NCSC[47]), siber konulardan sorumlu yetkili makamdır. NCSC, güvenlik açığı bildirimleri konusunda ise pasif bir tutum içerisinde ve gözlemci konumundadır. Açığı bulan kişi ile açığı düzeltecek olan arasındaki ilişkiye olabildiğince az müdahale olması gerektiği ve ancak gerekli hallerde konunun üçüncü taraflara raporlanabileceği savunulmaktadır. Daha çok, piyasanın doğal akışına uygun bir duruş sergilenmektedir [53].

3.4. İsrail

Başbakanlık Siber Daire Başkanlığına (National Cyber Bureau-(INCB)) bağlı Siber Olaylara Müdahale Ekibi (CERT-IL[48]), sivil bir girişim olarak ise IL-CERT[49] ve 8 üniversite[50] tarafından üyesi olunan Akademik IUCC CERT veya CERT-ILAN[51] siber olaylarla ilgili başlıca kurumlardır.

Güvenlik açığı yönetimi ile ilgili tanımlanmış ve kamuoyuna duyurulmuş süreçlerin varlığı tespit edilememiştir. US-CERT, NIST ve FIRST tarafından yapılan güvenlik bülten, duyuru ve düzenlemelerinden yararlanılmaktadır [54].

3.5. İngiltere

22 adet resmi ve özel siber olaylara müdahale ekibinin içerisinde CERT-UK kritik altyapılar başta olmak üzere ulusal çapta, GovCertUK ise kamu kurumlarından sorumlu olarak görev yapmaktadır [55]. GovCertUK, GCHQ[52]'nun bilgi ve güvenlikten sorumlu birimi olan CESG[53]'e bağlıdır.

Kamu ve özel sektör işbirliği iyi durumdadır. Ulusal kritik altyapıları korumak için 14 değişik sektörü bir araya getiren devlet kurumu olarak CPNI[54] oluşturulmuştur.

Güvenlik açığı yönetimi kapsamında, tespit edilen bir açığın ülke içerisinde raporlanmasını ve yönetilmesini sağlayacak bir yapı bulunmamaktadır.

[47] National Cyber Security Centre.
[48] Israel National Cyber Event Readiness Team.
[49] Israel's Computer Emergency Response Team.
[50] Bar-Ilan University, Ben-Gurion University of the Negev, Haifa University, The Hebrew University of Jerusalem, The Open University, Tel-Aviv University, The Technion-Israel Institute of Technology, The Weizmann Institute of Science.
[51] Israel's Academic Network Computer Emergency Response Team.
[52] (UK) Government Communications Headquarters.
[53] Communications Electronics Security Group.
[54] The Centre for Protection of National Infrastructure.

3.6. Rusya

Bilgi ve iletişim güvenliğine ilişkin köklü bir geçmişi olan Rusya'da, etkili siber güvenlik kurumları bulunmaktadır. Açık bilgi kaynaklarında bu kapsamda kısıtlı bilgiye ulaşılmışsa da, siber güvenlik konusunda resmi olarak görevlendirilmiş ve kamuoyuna duyurulmuş bir devlet kurumu olmadığı anlaşılmaktadır. Bu konudaki yetki ve eylemlerin büyük oranda başkanlık ve başbakanlık ofislerinde yoğunlaştığı görülmektedir [56].

Rusya'da kamuoyunca bilinen üç adet CERT birimi bulunmaktadır. Bunlardan birincisi ulusal çapta etkili devlet kurumu RU-CERT, ikincisi bir güvenlik şirketi bünyesinde faaliyet gösteren CERT-GIB ve sonuncusu WebPlusISP'dir [55].

Güvenlik açıkları yönetimine ve raporlanmasına dair faaliyet gösteren bir kuruluş veya mekanizmanın varlığı tespit edilememiştir.

3.7. İspanya

Toplam 16 adet askerî, sektörel ve akademik CERT içerisinde ulusal olarak yetkili ve sorumlu olan üç adet siber olaylara müdahale ekibi bulunmaktadır. Bunlar sırasıyla İstihbarat ve Kriptoloji birimine bağlı CCN-CERT, Siber Güvenlik Enstitüsüne (INCIBE) bağlı CERTSI ve kritik altyapılardan sorumlu CNPIC[55] bünyesindeki INTECO-CERT olarak sıralanmaktadır.

CCN-CERT; Ulusal Kriptografi Merkezi altında 2006 yılında kurulmuştur. Kamu kurumlarının ve stratejik diğer kurumların gizlilik dereceli bilgi sistemlerini korumak maksadıyla çalışmaktadır. Aynı zamanda ulusal uyarı ve müdahale merkezidir. CERT'ler arasında koordinasyonu kurmaktadır.

CERTSI daha çok iş dünyasına ve sivil kuruluşlara yöneliktir. Güvenlik bilgilendirme ve uyarılardan yaygın olarak sorumludur. Bilgi kaynakları arasında CERT, ISS-XForce ve Security Focus bulunmaktadır [57].

NIST ile INCIBE arasındaki anlaşma kapsamında NVD sayfasındaki güvenlik açığı verileri İspanyolca olarak da duyurulmaktadır. Bu durum, konuya ilişkin olarak ilk ve tek örnek olma özelliğini taşımaktadır. NVD'de bulunan İspanyolca güvenlik açığı verileri INCIBE tarafından İngilizceden çevrildiği için NVD'de o an mevcut bulunan açık sayısı ile örtüşmeyebilmektedir.

Güvenlik açıklarıyla ilgili görevlendirilmiş müstakil bir birim, özgün bir yapı veya mekanizma bulunmamaktadır.

[55] National Centre for Critical Infrastructure Protection.

3.8. Estonya

Bilişim altyapısı ve kullanım yaygınlığı ile önde gelen ülkelerden biri olan Estonya bunun karşılığını ironik bir şekilde kendisine yöneltilen 2007 siber saldırıları ile almıştır. Estonya, bu olayların hemen sonrasında siber stratejisini yayımlayarak kurumlarını sorgulayan ve yeniden kurgulayan ilk ülkelerdendir.

Estonya'nın, NATO Siber Savunma Mükemmeliyet Merkezi'nin de (CCD CoE) Talin'de kurulmasıyla birlikte Siber Güvenlik alanında bir bilgi ve cazibe merkezi haline geldiği ifade edilebilir. Siber güvenlik alanında resmi kurumlar ile özel sektör arasında yakın bir işbirliği ve koordinasyon bulunmaktadır. Ulusal siber olaylara müdahale ekibi, Bilgi Sistemleri Otoritesine[56] bağlı olarak çalışan CERT-EE'dir [58].

Tespit edilen bir yazılım güvenlik açığının ülke içerisinde raporlanabildiği ve süreç dâhilinde yönetildiği bir teşkilatlanma bulunmamaktadır.

3.9. Fransa

Siber güvenlik konusunun ciddi olarak ele alındığı örneklerden birisidir. Konuyla ilgili yetkili ve sorumlu makam Ulusal Bilgisayar Güvenliği Ajansıdır (ANSSI[57]). Değişik sektörlere dönük olarak toplam 16 adet CERT varsa da CERT-FR[58] ve CERT-IST[59] ulusal ölçekte sorumludurlar. CERT-FR, kamu kurumlarına yapılacak bir siber saldırıyla ilgilenirken, CERT-IST ise özel sektöre ve iş dünyası içerisinde bilgilendirme, koordine ve müdahale görevlerini yürütmektedir.

CERT-IST aynı zamanda güvenlik açığı yönetimi görevini üstlenmiştir. Tablo 2'de de görüleceği üzere Japonya hariç olmak üzere incelenen diğer ülkelerin aksine, açıkları yönetme işi Fransa tarafından önemsenmiş, kurumsallaşmış ve derli toplu bir biçimde ele alınmıştır. CERT-IST, açığı tespit eden kişiyle üretici arasında koordinatörlük yapmakta, aynı zamanda CERT-FR vasıtasıyla güvenlik duyurularını yayımlamaktadır.

IV. TÜRKİYE'DEKİ DURUM

4.1. Paydaşlar

Türkiye'de siber güvenlik konusunda ana koordinatör ve yetkili makam Ulaştırma, Denizcilik ve Haberleşme Bakanlığıdır. Bakanlık bu görevini, Siber Güvenlik Kurulu ve Bilgi Teknolojileri ve İletişim Başkanlığı

[56] Riigi Infosüsteem Amet: (Information Systems Authority), https://www.ria.ee/.

[57] Agence nationale de la sécurité des systèmes d'information.

[58] http://www.cert.ssi.gouv.fr/ .

[59] Le CERT dédié à la communauté Industrie, Services et Tertiaire, http://www.cert-ist.com/.

(BTK) vasıtasıyla yürütür. Bünyesinde, Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) bulunmaktadır.

Tablo 2: ABD Dışındaki Ülkelerin Siber Yetenekleri.

S.N.	ÜLKE	Siber Güvenlik Stratejisi	Siber Güvenlik Altyapısı	Siber Olaylara Müdahale	Bilgilendirme Duyuruları	Ulusal/Uluslararası İşbirliği	Güvenlik Açıkları Yönetimi	AÇIKLAMALAR
1.	Japonya	+	+	+	+	+	+	CVE Yönetim Kurulu
2.	Almanya	+	+	+	-	+	-	
3.	Hollanda	+	+	+	-	?	-	
4.	İsrail	+	+	+	+	+	-	
5.	İngiltere	+	+	+	-	-	-	
6.	Rusya	?	-	+	-	-	-	
7.	İspanya	+	+	+	+	+	-	NIST ile NVD Protokolü
8.	Estonya	+	+	+	-	+	-	CCD CoE
9.	Fransa	+	+	+	+	+	+	

USOM web sayfasının, diğer ülkelerdeki benzer kurum sayfalarına kıyasla yenilikçi bir tasarım ve faydalı içeriğe sahip olduğu görülmektedir. Bu sayfada, 2014 yılı sonlarına kadar (TÜBİTAK) Ulusal Bilgi Güvenliği Kapısı'ndan[60] yayımlanan duyurulara benzer şekilde güvenlik uyarı ve bilgilendirmeleri, ortalama ayda bir defa olacak şekilde yapılmakta, konuyla ilgili bilgi belge ve doküman bu yolla paylaşılmaktadır. Bu sayfadan güvenlik açıkları da belirli bir oranda duyurulmaktadır. Ne var ki ABD'deki NVD ve diğer bazı ülkelerle (Japonya, İsrail, İspanya vb.) kıyaslandığında bu duyuruların yeterli olduğunu söylemek güçtür.

Önde gelen paydaşlar arasında; kamu kurumları, bilişim firmaları ve İnternet Geliştirme Kurulu gibi girişimlerin dışında, erişim sağlayıcılar ve bu sektörün meslek kuruluşu Erişim Sağlayıcıları Birliği de ayrıca sıralanabilir.
Türkiye'de olası bir güvenlik açığı ekosistemine dâhil olması muhtemel paydaşlar, Tablo 3'de gösterilmiştir. Birinci dereceden ilgili ve süreçte etkili olacağı değerlendirilen kurumlar, tabloda koyu renkli olarak işaretlenmiştir.

4.2. Mevzuat ve Düzenlemeler

Türkiye'de siber güvenlik faaliyetleri 2006-2010 Bilgi Toplumu Stratejisi Eylem Planı ve bu planın 88. maddesine dayanarak TÜBİTAK tarafından yürütülen çalışmalarla büyük oranda hız kazanmış, sonrasında 2013-2014 Siber Güvenlik Stratejisi'nde yer alan 29 adet eylem maddesi ile ivmelenmiştir. Söz konusu Strateji güncellenerek 2016-2019 yıllarını kapsayacak şekilde 2016 yılı Nisan ayı içerisinde yeniden yayımlanmıştır. *"Siber güvenlik alanında uluslararası rekabet gücüne sahip bir ekosistemin oluşması"* vizyonuyla hazırlanan strateji belgesinin eylem planı bölümü bu kez kamuoyuna duyurulmamıştır.

Tablo 3: Türkiye'de Güvenlik Açığı Konusunda Muhtemel Paydaşlar.

Başbakanlık	MSB	MEB
Ulaştırma, Denizcilik ve Haberleşme Bakanlığı	Bilim, Sanayi ve Teknoloji Bakanlığı	Gümrük ve Ticaret Bakanlığı
BTK/USOM	SGE/TÜBİTAK	İçişleri Bakanlığı
TSK Siber Savunma Komutanlığı	Jandarma Genel Komutanlığı	EGM (Siber Suçlar Daire)
TSE	MİT	Enerji Bakanlığı
Siber Güvenlik Şirketleri	Savunma Sanayi Şirketleri	Yazılım Şirketleri
Üniversiteler, Enstitüler	Servis Sağlayıcılar	Adalet Bakanlığı
Türkiye Barolar Birliği	Noterler Birliği	Güvenlik Açığı Avcıları
Bilişim Tek. Derneği	Bilgi Güvenliği Derneği	…

Söz konusu dokümanlar; kapsamı, içeriği ve niteliği bakımından tartışılabilir olsa da mevzuat geliştirme ve organize olma konusunda süratli bir şekilde mesafe alınabildiğinin işaretleridir. Alınan kararların ve yapılan planlamaların hayata geçirilmesi konusunda aynı mesafenin kat edilebildiğini söylemek ise zordur. Buna çarpıcı bir örnek olarak 2013-2014 Eylem Planı'nın ikinci maddesinde Türk Dil Kurumuna verilen, siber güvenlik terminolojisinin ve sözlüğünün oluşturulması gibi somut, sınırları belli, erişilebilir ve görece basit bir hedefin dahi süreç içerisinde hayata geçirilememesi verilebilir.

Kritik altyapılar, eğitim ve farkındalık gibi hususların öne çıktığı 2013-2014 Eylem Planı'nın 10'uncu Maddesinde, "Yazılım Güvenliği Programının Yürütülmesi" görevinin TÜBİTAK sorumluluğunda çalışılması öngörülmüştür. Yazılım güvenliği konusu ayrıca, İnternet Geliştirme Kurulu Teknik Araştırmalar ve Standartlar Çalışma Grubu'nun altındaki Yazılım Güvenliği ve Standartlarının Belirlenmesi alt çalışma grubunda da çalışılmaktadır.

2013-2014 Eylem Planı'nda açıkça zikredilmese de planın 12. maddesi gereği TSE tarafından Açıklık

[60] http://www.bilgiguvenligi.gov.tr/ .

Bildirim Programı başlatılmıştır. Türkiye'de siber güvenlik hazırlık ve yetenek düzeyinin genel ortalamasına bakıldığında, güvenlik açıklarının yönetilmesini öngören bu eylem, yerinde, gerekli ve bilinçli bir girişim olarak görülmektedir. Bununla birlikte programın bazı yetersiz, eksik ve yanlış yönleri bulunmaktadır.

4.3. TSE Açıklık[61] Bildirim Programı

TSE Açıklık Bildirim Programını açıklayan dokuz sayfalık düzenleyici doküman 19 Haziran 2015 tarihinde yayımlanmıştır. Dokümanın hazırlanmasında, dünyada bu konuda belirleyici standartlar olan, güvenlik açıklarının nasıl ele alınacağına (ISO/IEC29147:2014) ve ne şekilde duyurulacağına (ISO/IEC30111:2013) dair düzenlemelere ve bu makalede incelenen dinamiklere büyük oranda yer verilmediği anlaşılmaktadır.

Programın tasarımına ve genel yaklaşımına bakıldığında; iyimser bir bakışın ve iyi niyet ile gönüllük esasıyla güvenlik açıklarının raporlanacağı varsayımının hâkim olduğu görülmektedir. Programın nasıl çalıştırılacağına, zorlayıcı tedbirler veya teşviklerin neler olacağına dair açıklayıcı hususlar bulunmamaktadır. Dünyada olup bitenler, yazılım güvenlik açıklarının yönetimi ile ilgili gösterilen üst düzey çaba, işletilen mekanizmalar ve süreçlere hemen hemen hiç değinilmediği gözlenmektedir.

Program dâhilinde ayrıca ulusal bir veri tabanı oluşturulması ve raporlanan güvenlik açıklarının burada kayıt altına alınması hedeflenmiştir. Bu maksatla hizmete sunulacağı belirtilen Açıklık Portalına[62], duyurulduğu günden itibaren erişim sağlanamamaktadır. Doküman içerisinde konuya ilişkin herhangi bir geçici madde, açıklayıcı bilgi veya şerh de bulunmamaktadır. Dokümandaki editoryal hatalar, eksik veri, kavram ve terimlere ilişkin değerlendirmeler bu makale kapsamında ele alınmamıştır.

TSE'nin siber güvenlik konularına eğilmesinin, siber alana ilgi duymasının ve bu kapsamda Açıklık Bildirim Programı gibi görevler almasının son derece isabetli olduğu ve bu gayretlerin desteklenmesi gerektiği değerlendirilmekte, Açıklık Bildirim Programı düzenleyici dokümanının sonraki sürümlerinin ise olgunlaştırılması sonrasında yayımlanmasının uygun olacağı düşünülmektedir.

4.4. Diğer Yetenek ve Girişimler

Konuya ilişkin olarak ülke içerisinde karşılıklı iletişim ve etkileşimi artıran faaliyetlerin çoğalmakta olduğu görülmektedir. Kamu, özel sektör veya ilgili diğer paydaşlarda, bu konuları yüz yüze tartışma, yeteneklerin neler olduğunu net olarak ortaya koyma, yetki ve sorumlulukları paylaşma ile gelişme kaydetme isteği ve gayreti bulunmaktadır. Türkiye'de bu kapsamda özellikle 2013 yılı sonrasında öne çıkan faaliyetlere; Kamu Bilişim Zirvesi, Bilişim Teknolojileri Standartları Toplantısı, Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansları, NopCon Hacker Buluşmaları, Hacktrick, Cypsec, IS'CyDeS ve daha fazlası örnek olarak verilebilir.

Bunların haricinde; dernek, şirket, okul, kurum vb. çatısı altında yoğunlaşan çalışmalar kapsamında; yetenek avcılığı, eğitim ve yetenek geliştirme alanlarında önemli girişimler vardır. TÜBİTAK, TSE gibi devlet kurumları ve diğer güvenlik şirketleri ile kâr amacı gütmeyen organizasyonların konuya ilişkin verdikleri eğitimler, icra edilen CTF[63] yarışmaları, siber kamplar vb. bu girişimler arasındadır.

Diğer taraftan güvenlik yazılımları, bilişim hizmetleri ve teknoloji danışmanlığı şirketlerinin de son dönemde yaptıkları yatırımlar ve ortaya koydukları ürünlerle, siber güvenliği öncelikli bir konu olarak ele aldıkları açıktır. Bunlar arasında; HAVELSAN tarafından Siber Savunma Teknoloji Merkezi'nin, STM tarafından ise Siber Füzyon Merkezi'nin kurulması, SignalSEC ve BGA[64] gibi şirketlerin SOME olarak yurt dışında akredite olmaları sıralanabilir.

Siber Güvenlik alanında Türkiye'deki mevcut eyleme geçme halini, dinamizmi, genç ve yaratıcı insan kaynağını daha verimli kullanmak adına bu çalışmaların organize olma durumunun, kurumsallığının, kapsamı ve niteliğinin artırılmasının uygun olacağı değerlendirilmektedir. Kapasite artırmaya yönelik çalışmaların içerisinde en önde geleni ise ulusal bir yazılım güvenlik açığı yönetim altyapısının tüm paydaş ve süreçleriyle kurulması olduğu düşünülmektedir.

Güvenlik açığı bulma konusunda kamuoyuna yansıyan veya yansımayan bireysel başarı hikâyeleri ile konuya merak ve birikimdeki artış Türkiye'nin bu alana ciddi olarak eğilmesi gerektiğinin küçük fakat önemli işaretleri olarak görülmelidir.

V. TÜRKİYE'DE GÜVENLİK AÇIĞI YÖNETİM SİSTEMİ MODELİ ÖNERİSİ

Yukarıda detayları açıklandığı üzere; güvenlik açığı ekosistemi içerisinde hangi aktörün, hangi rolü üstlendiği ve ne tür eylemler içerisinde bulunduğu Tablo 4'de gösterildiği gibi kolaylıkla tanımlanabilecek

[61] TSE tarafından resmi olarak tercih edildiği için "Açıklık" tabiri değiştirilmeden kullanılmıştır. Makale kapsamında kullanılan ifade "Güvenlik Açığı" veya "Açık"tır.

[62] https://siberguvenlikacikliklari.gov.tr

[63] Capture The Flag

[64] Bilgi Güvenliği Akademisi

bir konu değildir. Ancak temel olarak; aktörlerin kimler olduğu ve süreçte hangi rollerin sergilendiği bellidir. Dolayısıyla, bu konuda kurulacak yapı için aşağıdaki tablo bir referans olabilir.

Tablo 4: Aktörler ve Roller.

AKTÖR	ROL							
	Açığı Yaratıcı	Bulucu	Satıcı	Alıcı	Duyurucu	İstismar Kullanıcı	Yama	Kural Koyucu
Yazılım Şirketi	+	+	-	+	+	-	+	+
Güvenlik Açığı Avcıları	+	+	+	-	+	+	-	-
Güvenlik Yazılım Şirketleri	-	+	+	+	+	+	-	+
Güvenlik Açığı Müşterileri	-	-	-	+	+	+	+	+
Güvenlik Haber Kaynakları	-	+	+	+	+	-	-	+
Düzenleyiciler	-	-	-	-	+	-	-	+

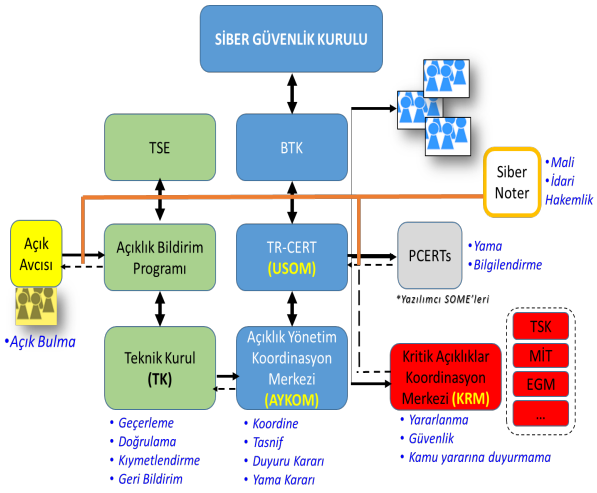
Makalenin önceki bölümünde incelenen ülkelere bakıldığında, sürecin genelde üç ana başlıkta işlediği anlaşılmaktadır:

Birincisi; yönetim, koordinasyon, standartları belirleme, işbirliğini artırma, duyuru, farkındalık ve bilgilendirme için ulusal çapta yetkili bir otoritenin varlığıdır. *İkincisi*; güvenlik açıklarını teknik olarak analiz etmek, incelemek ve kıymetlendirmek için birikimli, bilimsel yönü ağır basan ulusal çapta bir oluşumdur. *Üçüncüsü* ise kritik altyapıları korumak, milli kritik sistemleri gözetmek ve gerektiğinde kıymetli açıklardan yararlanabilmek için ulusal bir bilgi paylaşım ve reaksiyon ağını da içeren bir yapılanmadır.

Her üç boyutu da ele alarak Türkiye için önerilen örnek model Şekil 7'de sunulmuştur. Model büyük oranda, mevcut durum ve düzenlemeler ile hâlihazırda kurumlar tarafından kazanılmış yetenekler ve yüklenilen sorumluluklar üzerine kurgulanmıştır.

Anlaşılırlığı azaltabileceği için Şekil 7'de, olası diğer aktörler ve sürece dair detay işlemlere yer verilmemiştir. Kurulacak sistemin sağlıklı işleyebilmesi için; yöntemsel, idari, mali ve teknik konuların olabildiğince ayrıntılı tanımlanması, yetki, sorumluluk ve kurallarının net bir şekilde ortaya konulması uygun olacaktır. Bunun haricinde kurumsal ve sektörel SOME'lerin sayısı artırılarak aralarındaki bilgi paylaşımı ve koordinasyonu geliştirecek tedbirler alınmalıdır.

Şekil 7'de gösterilen güvenlik açığı yönetim süreci önerisi, temel aktörleriyle ve işleyişiyle aşağıda açıklanmıştır.



Şekil 7: Türkiye Güvenlik Açığı Yönetim Sistemi Modeli Önerisi (Örnek)

5.1. Açığı Bildirme ve İlk İşlem

Güvenlik Açığı Avcısı, herhangi bir yazılımda, bir web sayfasında veya uygulamada tespit etmiş olduğu açığı TSE Açıklık Bildirim Programı kapsamında faaliyete geçmesi öngörülen **Açıklık Portalı** üzerinden raporlamalıdır. "Avcı"nın Dünya'nın herhangi bir yerindeki bir şahıs olabileceği öngörüsüyle, Açıklık Portalı mutlaka başta İngilizce olmak üzere diğer yabancı dillerde de tasarlanmalıdır.

Teknik Kurul tarafından, raporlanan "aday" güvenlik açığının, belirlenmiş bir süre içerisinde inceleneceğine ve sonucunun bildirileceğine dair açık avcısına geri dönüş yapılmalıdır.

5.2. Açığı Analiz ve İnceleme

Teknik Kurul, bir nevi CVE Editörler Kurulu olarak düşünülebilir. Üyeleri; yazılım güvenlik açıkları konusunda ileri düzeyde teknik bilgi ve beceriye sahip ve alanda uzman kişilerden seçilmelidir. Teknik Kurul, kurum temsilcilerinin yanında, bağımsız çalışan bireylerden de oluşabilir. TÜBİTAK Siber Güvenlik Enstitüsü'nün (SGE), birikimi ve altyapısı ile Teknik Kurul'un merkezini teşkil edebileceği değerlendirilmektedir.

Kurulun üyeleri; daimi ve geçici olmak üzere iki grupta tasnif edilebilir. Daimi üyeler; kamu kurumu veya kâr amacı gütmeyen kuruluşlardan (Örn: SGE, TSE, MİT,

TSK, Jandarma, EGM[65], BGD[66], Üniversiteler vb.) seçilmeli, güvenlik açığının niteliğine ve hangi yazılımda olduğuna bağlı olarak geçici üyelerden de (Örn.: BGA, savunma yazılımları şirketleri, siber güvenlik şirketleri, yazılım şirketleri vb.) yararlanılabilmelidir.

Teknik Kurul tarafından, iletilen açığın iddia edildiği gibi bir güvenlik sorunu yaratıp yaratmadığı, benzer bir ortam yaratılmak suretiyle denenmeli ve doğrulanmalıdır. Açığın temel sebebi ve bu sebepten etkilenmiş diğer yazılımlar olup olmadığı analiz edilmelidir. Geçici üye olarak; güvenlik açığı bulunan yazılımın şirket temsilcisi, talebe bağlı olarak çağrılıp bilgisine başvurulabilir. Kendisine güvenlik açığı konusunda bilgi verilebilir. Teknik Kurul işlemlerine daimi veya geçici olarak dâhil olan üyelerin güvenlik açık bilgisinin gizliliğini korumaları sağlanmalıdır.

İnceleme sonucunda güvenlik açığı doğrulanırsa, söz konusu açığın hangi ciddiyette bir güvenlik durumu yaratabileceği değerlendirilmeli ve puanlanmalıdır. Eğer güvenlik açığı milli kritik sistemlerde ve kritik altyapılarda ciddi bir etki yaratma potansiyeline sahipse, isimlendirme sırasında bu durum için ayrı bir kodlama şekli öngörülmelidir. Bu safhanın son aşamasında, uygun şekilde etiketlenen güvenlik açığı için açığı tespit eden kişiye kurul tarafından takdir edilen bir ödül verilmesi (ücret ödenmesi vb.) uygun olacaktır.

"Avcı" tarafından tespit edilen açığın, doğrudan üreticiye veya diğer platformlara raporlanmasının engellenmesi maksadıyla ekonomik teşvik ve yasal zorunluluk boyutları önem kazanmaktadır. Bu nedenle, TSE koordinesinde yürütülecek bu faaliyet için piyasa şartlarına uygun bir bütçe ayrılması ve gerekli yaptırımların mevzuat ile düzenlenmesi gerekir. Bu noktada ayrıca, güvenlik açığını bulan kişinin değişik kaygılarla kimliğini açık etmeme tercihi anlayışla karşılanmalı ve buna uygun tedbir alınmalıdır. Bu tedbirler kapsamında; anonim bir aktöre, bitcoin vb. uygun yöntemlerle ödeme yapılmasına imkân tanıyan düzenlemeler de düşünülmelidir. Sürecin otomasyonla işletilmesi, ayrıca; idari, mali ve hukuki taahhütlerin bu makalede önerilen **Siber Noter**lik birimi tarafından gözetilmesinin uygun olacağı düşünülmektedir.

5.3. Değerlendirme, Yama ve Duyuru Kararı

Uygun biçimde isimlendirilen ve etiketlenen güvenlik açığı başka herhangi bir işleme tabi tutulmaksızın USOM bünyesinde teşkil edilebilecek **Açıklık Koordinasyon ve Yönetim Merkezi**ne iletilmelidir. Burada güvenlik açığının hangi işleme tabi tutulacağı (yama, duyuru, saklama vb.), yama yapılacaksa duyuru öncesi üretici kuruluşa bu açığı kapatmak için ne kadar süre verileceği, kamuoyuna ne zaman duyurulacağı, duyurulmama tercihinin kullanılıp kullanılmayacağı gibi kararlar verilmelidir. Merkez tarafından bütün bu görevler, Siber Güvenlik Kurulu adına ve kurul yetkileriyle ifa edilebilir, aynı zamanda sekretarya vb. görevleri de bu merkez vasıtasıyla yürütülebilir.

Bu konuda ayrıca; güvenlik açığı bulunan yazılımın kullanıldığı kritik sistem ve altyapılardan sorumlu olan kurumların açıktan haberdar edilebilmesi için, bu kurumlar tarafından kullanılan yazılım envanter bilgileri, USOM tarafından güncel bir şekilde tutulmalı, Teknik Kurul ve ilgili diğer paydaşlarla paylaşılmalıdır.

USOM'un görevleri içerisine ayrıca, bu kapsamdaki yeteneklerin tespiti ve yetkinliğin artırılması maksadıyla, ülke sınırları içerisinde icra edilecek bütün güvenlik açığı yarışma ve teşvik programlarının genel koordinatörlüğü, sponsorluğu veya gözetimi de dâhil edilebilir.

5.4. Çalışma Alanlarına İlişkin Diğer Öneriler

Yukarıda önerilen organizasyonda, prensip olarak, merkezi yapının mümkün olduğunca dar bir paydaş grubu ile sınırlandırılmasının, bilgilendirme, farkındalık, destek, işbirliği ve haberleşme ağlarının ise olabildiğince geniş tutulmasının uygun olacağı düşünülmektedir.

Siber Olaylara Müdahale Ekipleri (SOME) olarak ifade edilen birimlerin yetki ve sorumluluklarının netleştirilmesine, "müdahale" sözcüğünün bu kurumlara yüklediği görevin karşılığı çok iyi tanımlanarak, kolluk kuvvetlerinin yetki alanına girilmemesine özen gösterilmesi faydalı olacaktır.

Ödül ve teşviklerin artmasıyla, yazılım geliştiriciler tarafından, kodların içerisine kasten yerleştirilmesi olası açıkların önüne geçmek için, güvenlik açığını bulma karşılığında verilecek teşvik miktarının, yazılımın o bölümünü geliştiren programcıdan tahsil edilmesi yoluna gidilerek bir ölçüde caydırıcılık sağlanabilir.

Yama üretimi ve yamanın tatbik edilmesinde yaşanan gecikme ve ihmallerin önüne geçmek maksadıyla, süreci hızlandırıcı (oto güncellemenin varsayılan standart olması, yama uygulama miatlarının belirlenmesi vb.) kurumsal ve ulusal tedbirler alınmalıdır. Ancak, bu ifadeden, yamanın ne olursa olsun bir an önce yapılmasının her durumda gerekli ve geçerli olduğu anlamı çıkarılmamalıdır. Özellikle kritik sistemlerde kullanılan yabancı kaynaklı ticari ve güvenlik yazılımlarının; kriz, gerginlik ve çatışma dönemlerinde yayımlanan yamalarına temkinli

[65] Emniyet Genel Müdürlüğü
[66] Bilgi Güvenliği Derneği

yaklaşılmalıdır. Uygulanan her bir yamanın, kasten veya kazara yeni bir güvenlik açığı veya servis dışı bırakma durumu yaratabilme olasılığı dikkate alınmalıdır.

Genelde büyük ve yaygın yazılımlar için kullanılan bir yöntem olan "son kullanma tarihi" uygulamasının tüm yazılımlar için geçerli bir kural olarak benimsenmesi faydalı olacaktır. Böylelikle kullanıcılar, hangi tarihten itibaren artık o ürünün yazılım üreticisi tarafından desteklenmeyeceğini bilmek suretiyle gerekli tedbirleri alabileceklerdir. Yazılım güvenlik açıklarının değeri ve önemi bilinmekle birlikte, yazılımların sayısı ve karmaşıklığı ile siber ortama bağımlılığın artmasıyla birlikte ileride çok daha fazla önem kazanacağı açıktır. Bu konunun, milli bir mesele olarak gizlilik boyutları olabileceği göz önüne alınmalıdır.

Güvenlik açığı yönetiminde, açık bilgisine ulaşma, onu istismar etme veya ciddi bir hasar yaratmadan önce açıklığı kapatma konusunda amansız bir yarış vardır. Öyle ki, savunma bütçesi yaklaşık olarak, dünyadaki diğer bütün ülkelerin savunma harcamalarının toplamına eşit olan [59] ABD Savunma Bakanlığı tarafından bile, sistemlerindeki güvenlik açıklarını tespit etmek için bir yarışma düzenlenmiştir [60]. Bu yarışmada 90 adet güvenlik açığına karşılık araştırmacılara ödül olarak 75.000 dolar dağıtılmıştır [61].

Benzer şekilde, kritik sistemlerde ve altyapılarda kullanılan yazılımlar için, sistemleri kullanıma almadan önce geniş katılımlı kara kutu (black box) testleri yapılması uygun olacaktır. Konuya ilişkin olarak; devlet, üniversiteler/araştırma kuruluşları ve özel sektörün bir araya gelerek yaratacağı sinerji ile Türkiye'nin siber kapasitesi gelişecektir. Sekiz milyon nüfusu ve son derece kısıtlı doğal kaynaklarına rağmen yıllar içerisinde bir "siber süper güce" dönüşebilen İsrail, bu anlamda örnek alınabilir [62].

Yazılım güvenlik açıklarıyla en yakından ve doğrudan ilgili sektör, antivirüs yazılım üreticileri ve siber güvenlik şirketleridir. Güvenlik açığı ekosistemi içerisindeki bir kümelenme ile kazanılabilecek yetenekler, küresel çapta bilinirliği olan ulusal bir antivirüs yazılım markası geliştirilmesi ve Türkiye menşeli bir siber güvenlik şirketi yaratılmasının yolunu açabilir. Rusya'da kurulan ve dünya çapında dev bir markaya dönüşen Kaspersky, böylesi bir girişim ve iş modelinin en somut örneğidir [63].

VI. SONUÇ VE DEĞERLENDİRMELER

Yazılım firmaları, normalde tam zamanlı eleman çalıştırarak yapamayacakları büyüklükte ve önemde işleri, güvenlik açığı bulma teşvik programları ve 0-gün açığı pazarları sayesinde yapabilmekte, normalde sahip olamayacakları ölçüde yetenekleri bu yolla kazanabilmektedir. Hizmetleri karşılığı güvenlik açığı avcılarına verilen ücretler görece tatmin edici olsa da, ödül için ayrılan miktarlar, büyük ölçekli firmaların bilançolarında çok fazla bir anlam ifade etmemektedir. Örneğin Facebook tarafından, 2015 mali yılı için 18 milyar dolar gelir açıklanırken [64], teşvik programları üzerinden açık avcılarına o yıl için sadece 936.000 dolar dağıtıldığı duyurulmuştur [30].

Bu anlamda yazılım açığı avcılarına ödenen bedeller aslında kamu veya özel sektör kuruluşları için küçük boyutlardadır. Dolayısıyla, teşvik mekanizmaları kurma ve güvenlik açığı yönetim altyapısını oluşturma konularında başta kamu olmak üzere etkin diğer aktörler tarafından harekete geçildiği takdirde ülke için bir avantaj yaratabilme fırsatı bulunduğu değerlendirilmektedir.

Küresel ölçekte olaya bakıldığında; işin büyüklüğü, karmaşıklığı ve dinamikliği görüldükçe, güvenlik açığı yönetimi konusunda ulusal bir ekosistemin oluşturulması, ulaşılması zor bir hedef olarak değerlendirilebilir. Ancak, iyi incelenmiş, tutarlı, milli kritik sistemleri önceliğine alan mekanizma, süreç ve kurallar doğru kurgulandığı takdirde, hem ülkenin konuya ilişkin kaynak ve kapasitesinin artacağı, hem de zaman içerisinde bu alanda yaşanması muhtemel ağırlık merkezi kaymalarında Türkiye'nin, güvenlik açığı yönetiminde birikimli ve güvenilir bir seçenek olarak devreye girebileceği düşünülmektedir.

2015 yılı ITU Küresel Siber Güvenlik Endeksine göre, ABD'nin 0,824 puanla birinci olduğu bir listede, Türkiye 0,647 puanla 7'nci sırayı İsveç ve Letonya ile birlikte paylaşmıştır. Söz konusu indeksin oluşturulması ve puanlanmasında ülkeler; yasal, teknik, kurumsallaşma becerisi, yetenek geliştirme ve uluslararası işbirliği olmak üzere beş boyutta değerlendirilmektedir. Türkiye özellikle kurumsallaşma becerisi boyutunda aldığı puanla öne çıkmaktadır.
Türkiye'nin, siber alanda organize olma konusunda güçlü bir ülke olduğu değerlendirilmektedir. Alınan kararları ve öngörülen mekanizmaları hayata geçirme, karşılıklı güveni tesis etme ve sürdürme yönleriyle ise geliştirmeye muhtaç taraflar bulunduğu düşünülmektedir. Buna bir örnek olarak, 2016 yılında icra edilen Kamu Kurumları Bilişim Zirvesinde, EGM temsilcisi tarafından, kamu kurumlarından son iki yıldır hiç bir siber suç duyurusu iletilmediği, ortak çalışma imkânlarının oluşmadığı, hatta bazen herhangi bir kuruma saldırıya uğradığı ikazında bulunduklarında bile yeterli işbirliği imkânını sağlayamadıklarını ifade etmesi verilebilir [65].

NVD üzerinden kamuoyuna duyurulan yaklaşık 76.500 güvenlik açığının belirli bir kısmının da Türkiye Cumhuriyeti vatandaşları tarafından bulunmuş olması doğal olarak beklenebilir. Tespit edilmiş olması muhtemel bu güvenlik açıklarına ilişkin bilginin yurt içinde tutulması ve yönetilebilmesi durumunda sağlayabileceği ekonomik, ticari, askerî ve istihbarî güç kıymetlendirilmelidir. Güvenlik açığı yönetimine eğilmemenin bir fırsat maliyeti bulunduğu değerlendirilmektedir.

Organik veya organik olmayan bağlar ile sistematik iletişim ve işbirliği imkânlarının oluşturulmasıyla; genç, yaratıcı ve yenilikçi insan kaynağı dinamikleri bu alana yoğunlaştırılabilir. Milli Eğitim Bakanlığı tarafından, ilköğretimden başlamak üzere bilgilendirme, farkındalık vb. yanında; yazılım geliştirme becerisi, algoritma yaratma ve güvenlik açığı bulma melekesi kazandırmaya yönelik eğitimlerin de müfredata dâhil edilmesiyle bu alandaki mevcut yetenek artırılabilir. Bu sayede Türkiye, zaman içerisinde bir çekim merkezi haline gelebilir.

Böylesi bir girişimin olumlu sonuçları kısa vadede gözlemlenmeyebilirse de bu yapının tesisi ve sürdürülebilirliğinin sağlanmasında büyük yarar bulunduğu değerlendirilmektedir.

KAYNAKLAR

[1] P.W. Singer & Allan Friedman, "Siber Güvenlik ve Siber Savaş", Buzdağı Yayınları, 2014.

[2] Mathhew Noyes & Robert Belk, "On the Use of Offensive Cyber Capabilities: A Policy analysis on Offensive US Cyber Policy", Office of Naval Research, 20 Mart 2012.

[3] Maj. Mark A. Cobos, "Nodes and Codes: The Reality of Cyber Warfare", US Army, 2012.

[4] Jordan Robertson, "Hackers Cross From Digital to Physical World", Taipei Times, 27 Ekim 2011.

[5] Kenneth Geers, "Strategic Cyber Security", CCD CoE, 2011.

[6] Chris Preimesberger, "Plugging Holes", eWeek, 2006.

[7] Richard A. Clark & Robert K. Kane, "Siber Savaş", 2010.

[8] Martin Libicki, Lillian Ablon, Tim Web, "The Defenders Dilemma: Charting a Course Toward Cybersecurity", RAND, 2015.

[9] Kod Satır Sayıları, "Codebases: Millions of Lines of Code", Information is Beautiful, 08/11/2016, http://www.informationisbeautiful.net/visualizations/million-lines-of-code/.

[10] Black Duck Open Hub, "Project Chromium (Google Chrome)", 10/05/2016, http://code.openhub.net/.

[11] Andreas Kuehn, Milton Muller, "Shifts in The Cybersecurity Paradigm: Zero Day Exploits, Discourse and Emerging Institutions", NSPW '14, New Security Paradigms Workshop, 63-68, 2014.

[12] USOM, Ulusal Siber Olaylara Müdahale Merkezi, 08/11/2016,https://www.usom.gov.tr/index.html

[13] CERT, Carneige Mellon University Software Engineering Institute, 08/11/2016, http://www.cert.org/faq/.

[14] FIRST, Forum of Incident Response and Security Teams, 08/11/2016, http://www.first.org/.

[15] Serge Egelman & Cormac Herloy,, "Markets for Zero Day Exploits: Ethics and Implications", Berkeley; Microsoft, 2013.

[16] Stefan Frei, "Security Econometrics, The Dynamics (In)security" Doktora Tezi, Zürih Teknoloji Enstitüsü, ETH, 2009.

[17] MITRE, "Corporate Overwiev",08/11/2016, www.mitre.org.

[18] CVE, Common Vulnerabilities and Exposures, "About", 08/11/2016, https://cve.mitre.org/about/

[19] CWE, Common Weakness and Enumeration, "About", 08/11/2016 https://cwe.mitre.org/about/.

[20] Hyun Joh, "Quantitive Analyses of Software Vulnerabilities", Doktora Tezi, Colorado Üni., 2011.

[21] NIST, "General Information", 08/11/2016, http://www.nist.gov/

[22] NVD, National Vulnerability Database, 08/11/2016, https://nvd.nist.gov/.

[23] CVSS, "Common Vulnerability Scoring System", 10/06/2015, https://www.first.org/cvss.

[24] CERT, "About Us", Carneige Mellon University, SEI, 08/11/2016, http://www.cert.org/about/.

[25] US CERT, "About Us", 08/11/2016, www.us-cert.gov/about-us.

[26] Danny Yadron, "FBI Confirms It Won't Tell Apple How It Hacked San Bernardino Shooter's iPhone", The Guardian, 28/04/2016.

[27] James Sanders, "How the Wassenaar Arrangement Threatens Responsible Vulnerability Disclosures", Tech Republic, 07/07/2015.

[28] Microsoft Bounty Programs, 08/11/2016, https://technet.microsoft.com/library/dn425036.

[29] Leyla Bilge, Tudor Dumitras, "Before We Knew It: An Emprical Study of Zero-Day Attacks in The Real World" Symantec Co., 2012.

[30] 2015 Highlight, "Facebook Bug Bounty", 09/02/2016, https://www.facebook.com/whitehat.

[31] Kenny Jake, "10-Year Old Cashes on Facebook Bug Bounty Program", Kaspersky Lab. Daily, 06/05/2016.

[32] CHIP Online, "Hack'leyen, ardından işe alınan 7 hacker!",Tarihsiz, www.chip.com.tr/galeri/hack-leyen-ardindan-ise-alinan-7-hacker_2220.html .

[33] Yaman Roumani ve diğ., "Time Series Modelling of Vulnerabilities", Journal Computers and Security, Cilt 51 Sayı C, Temmuz 2015, 32-40, Elsevier Advanced Technology Publications Oxford, UK, 2015.
[34] Security Experts: Eugene Kaspersky, Kaspersky Lab, 08/11/2016, http://www.kaspersky.com/.
[35] CyberMag Online, "Hacker Ekonomisine Daha Yakından Bir Bakış", 09/02/2016, http://www.cybermagonline.com/hacker-ekonomisine-daha-yakindan-bir-bakis/.
[36] Jeffrey Carr, "Inside CyberWarfare", O'Reilly, 2010.
[37] Hannes Holm, Khalid Khan Afridi, "An Expert-Based Investigation of the Common Vulnerability Scoring System", Computers & Security, 2015,18-30.
[38] Ozment Andy," Vulnerability Discovery & Software Security", University of Cambridge, Doktora Tezi, 2007.
[39] "OSVDB: FIN", OSVDB, Open Source Vulnerability Database, 05 Nisan 2016, https://blog.osvdb.org/2016/04/05/osvdb-fin/
[40] HackerOne: The Vulnerability Coordination & Bug Bounty Platform,8/11/2016, https://hackerone.com/
[41] A Guide For Anyone New To Vulnerability Reporting,08/11/2016, http://howdoireportavuln.com
[42] Community powered disclosure, 08/11/2016, http://disclosure.io
[43] Responsible Disclosure 08/11/2016, http://responsibledisclosure.nl/en/# ,
[44] Responsible Disclosure Guideline, 08/11/2016, www.ncsc.nl/
[45] CERT, What is Vulnerability Coordination?, 08/11/2016, Wiki, https://vuls.cert.org/ .
[46] CERT, "Vulnerability Disclosure Policy", Carneige Mellon University, Software Engineering Institute (SEI), 08/11/2016, http://www.cert.org/vulnerability-analysis/
[47] EFF, "Coders' Rights Project Vulnerability Reporting FAQ", Electronic Frontier Foundation, 08/11/2016, www.eff.org.
[48] Secunia, "Secunia Vulnerability Review 2015", 25/03/2015, https://secunia.com/?action=fetch&filename=secunia_vulnerability_review_2015_pdf.pdf
[49] JPCERT/CC, Japan Computer Security Incident Response Team Coordination Center, 08/11/2016, https://www.jpcert.or.jp/.
[50] IPA, Information Technology Promotion Agency, Japan, 08/11/2016, http://www.ipa.go.jp.
[51] EU Cybersecurity Dashboard. "A Path to a Secure European Cyberspace", Galexia, BSA, The Software Alliance, 2015.
[52] CERT-Bund, "Das Computer-Notfallteam des BSI", 08/11/2016, https://www.cert-bund.de/about.
[53] Nationaal Cyber Security Centrum, "Policy for Arriving at a Practice for Responsible Disclosure", Dutch Ministry of Security and Justice, 30/01/2013.
[54] CERT-IL, Israel National Cyber Event Readiness Team, 08/11/2016, https://cert.gov.il/.
[55] ENISA, CSIRTs by Country - Interactive Map, 08/11/2016, https://www.enisa.europa.eu/.
[56] Levin Avner ve diğ, Securing Cyberspace: A Comparative Review of Strategies Worldwide, Ted Rogers School of Management, Ryerson University, 2013.
[57] CERTSI, CERT de Seguridad de Industria, Vulnerabilidades, 08/11/2016, www.incibe.es/ .
[58] CERT-EE, Estonya Siber Olaylara Müdahale Ekibi, 08/11/2016, https://www.ria.ee/ee/cert.html.
[59] SIPRI, Military Expenditure Database, 08/11/2016, http://www.sipri.org/.
[60] DoD News, "'Hack the Pentagon' Pilot Program Opens for Registration" Defense Media Activity, 31 Mart 2016, http://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration.
[61] Sean Lyngaas, "Pentagon bounty program reveals 90 bugs", 17/05/2016, https://fcw.com/articles/2016/05/17/hack-the-pentagon.aspx .
[62] Homeland Security News Wire, "How Israel Became a Cybersecurity Superpower", 18/05/2016, http://www.homelandsecuritynewswire.com/dr20160518-how-israel-became-a-cybersecurity-superpower
[63] Shachtman Noah, "Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals",Wired Magazine, 23 Temmuz 2012, https://www.wired.com/2012/07/ff_kaspersky/
[64] Facebook, "Reports Fourth Quarter and Full Year 2015 Results", 27/01/2016, http://www.prnewswire.com/news-releases/facebook-reports-fourth-quarter-and-full-year-2015-results-300210893.html .
[65] Kamu Bilişim Zirvesi/Antalya, 14-16 Nisan 2016, 08/11/2016, http://www.cybermagonline.com/kamu-bilisim-zirvesinde-siber-guvenlik-konusuldu/