Journal of Human Sciences
ISSN: 2458-9489
Volume: 13 Issue: 3 Year: 2016

Evaluation ofthe most preferred operating systems oncomputers in terms of vulnerabilities

Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi

Aysun Coşkun[1]
Ümit Bostancı[2]

Abstract

Because it is one of the most fundamental programs running on the computer, operating systems, are known to provide security infrastructure for other programs and services that run on computer. Unless any precautions are taken against vulnerabilities on the operating system, the system becomes eligible to be exploited, it paves the way to achieve the target of attackers. Hence, remediation of vulnerabilities on the operating system is evaluated to be extremely significant. In this study, a new database was created by questioning vulnerabilities existing in the most widely used operating systems on desktop and laptop computers from National Vulnerability Database of the US and CVEDETAILS databases. With regard to these vulnerabilities, CVSS scoring system which is used for scoring them created by FIRST was examined, in the light of the of re-scoring of identified vulnerabilities, the analysis of security of the operating systems was done with quantitative methods. One of the most important element of cyber security, fundementals of vulnerabilities, and role in the exploitation of the vulnerabilities of the computers were explained. In this study recently occured cyber security incidents because of vulnerabilities were also examined, and information about vulnerabilities allowing attack in these events was collected. Consequently, considering hosting the vulnerabilities, it is aimed to assess the availability of the operating systems in terms of security.

Özet

Bilgisayar üzerinde çalışan en temel programlardan biri olması sebebiyle işletim sistemlerinin bilgisayar üzerinde çalışan diğer programlara ve servislere güvenlik altyapısı sağladığı bilinmektedir.İşletim sistemi üzerindeki güvenlik açıklıklarına karşı gereken önlemler alınmaz ise, sistem istismar edilmeye uygun hale gelmekte, bu durum saldırganlarınhedeflerine ulaşması için zemin hazırlamaktadır. Bu sebeple, işletim sistemlerinin üzerindeki güvenlik açıklıklarının kapatılmasının son derece önemli olduğu değerlendirilmektedir. Bu çalışmada bilgisayarlarda en çok kullanılan işletim sistemlerinde var olangüvenlik açıklıklarıABD'nin Ulusal Açıklık Veritabanı ve CVEDETAILS veritabanlarından sorgulanarak yeni bir veritabanı oluşturulmuştur.Toplanan açıklıklarla ilgili olarak FIRST tarafındanoluşturulmuş CVSS puanlama sistemiyle yapılan puanlamalar incelenmiş, tespit edilen açıklıkların yeniden puanlamaları yapılarak çıkan sonuçlar ışığında işletim sistemlerinin güvenlik açısından analizi nicel yöntemlerle yapılmıştır. Siber güvenliğin en önemli unsurlarından birisi olan güvenlik açıklıklarıyla ilgili temel hususlar ile açıklıkların bilgisayarların istismar edilmesindeki rolü ortaya konulmuştur. Çalışmada ayrıca; yakın geçmişte açıklıklar kullanılarak gerçekleştirilen siber güvenlik olayları incelenmiş, bu olaylarda saldırıya imkan sağlayan açıklıklarla ilgili bilgiler toplanmıştır. Sonuçta, barındırdığı açıklıklar dikkate alındığında, işletim sistemlerinin kullanılabilirliğinin güvenlik açısından

[1]Doç. Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Bilgisayar Eğitimi ABD, aysunc@gazi.edu.tr
[2] Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim ABD, umit.bostanci@hotmail.com

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

Keywords: Cyber security; information security; vulnerability;zero day vulnerability;operating system; critical infrastructure; exploit.

(Extended English abstract isat the end of this document)

Anahtar kelimeler: Siber güvenlik; bilgi güvenliği; açıklık, sıfırıncı gün açıklığı;işletim sistemi; kritik altyapı; istismar.

1.Giriş

Yaklaşık bir salon büyüklüğünde olan ve işlem yapmak için delikli kartlara ihtiyaç duyulan ilk bilgisayarlar, 20'nci yüzyılın ikinci yarısından sonra yaşanan teknolojik gelişmelerlebirlikte boyut olarak küçülürken, işlevleri açısından hayatın her alanında var olan, vazgeçilmez bir cihaz olarak insanoğlunun hayatında önemli bir yer tutmaya başlamıştır.İnternet kullanımının yaygınlaşmasıyla birlikte; bilginin işlenmesi, saklanması ve iletilmesi hususunda büyük kolaylık sağlayan bilgisayarlar vasıtasıyla zamana ve mekana bağlı kalmaksızın her türlü işlemi yerine getirmek mümkündür.Günümüzde akıllı telefon, tablet ve dizüstü bilgisayar kullanımı oldukça yaygınlaşmıştır.İnsanoğlu yanında taşıdığı bu mobil cihazlar vasıtasıylafatura ödemesi gibi basit işlemlerin yanı sıra, karmaşık bankacılık işlemlerini yapabilir ve hatta bir süper marketten alışveriş yapabilir duruma gelmiştir.

ARPANET olarak 1970'lerde sadece askeri kurumlar tarafından kullanılmaya başlayan İnternet, yaygınlaşıp, kişisel kullanıcılara açılmasıyla birlikte dünyanın her yerinde kullanılan bir teknoloji olmuştur.Uydu ve GSM teknolojisindeki gelişmeler, okyanusun ortasından Everest dağının tepesine kadar dünyanın herhangi bir yerindeki bilişim cihazı ile iletişim kurulmasını mümkün kılmıştır. Bilişim cihazlarının birbirleriyle haberleşmesini sağlayan internet teknolojisinin sunduğu altyapının yaygın olarak kullanılmasıylabirlikte "siber alan" kavramı ortaya çıkmıştır.

Kevin Ashton tarafından 1999 yılında yapılan bir sunumdakullanılmasıyla ilk defa gündeme getirilen "Nesnelerin İnterneti"(Internet of Things, IoT) teknolojisi(Ashton, 2009)ile İnternete bağlanancihaz sayısı her geçen gün artmakta,buna bağlı olarak siber alan her geçen gün genişlemektedir.Siber alan'a dahil olan bu yeni teknolojivasıtasıyla açıklıkların sayısında ciddi bir artış yaşandığı gözlemlenmektedir.Hemen hemen her alanda kullanılan bu elektronik cihazları yönetmek ve kontrol etmek için çeşitli yazılımlara ihtiyaç duyulmaktadır.Zira; üzerinde herhangi bir yazılım barındırmayan,sadece elektronik devrelerden oluşan bu aygıtlara işlem yaptırabilmek imkansızdır.Yazılımlar arasında en önemli olarak nitelendirilebilecek işletim sistemi, kullanıcı ile bilgisayar donanımı arasında bulunan, üzerinde çeşitli uygulama programlarının çalıştırılmasınaimkan sağlayan ve bilgisayar üzerindeki tüm işlemlerin kontrol edilmesinden sorumlu olan (Brookshear, 2012:124)temel bir yazılımdır.

Yönlendiricilerden, tablet bilgisayarlara kadarsiber alanda yoğun olarak kullanılan her cihazın üzerinde yüklü bir işletim sistemi mevcuttur.Sıradan kullanıcılara ihtiyaç duyduğu işlemleri kolaylıkla yapabilme imkanı sağlayan uygulama programları ise işletim sistemlerinin üzerinde çalışmaktadır.Bilgisayarların üzerinde çalışan gerek uygulama yazılımlarında ve işletim sistemlerinde, gerekse bilgisayarın donanım parçaları üzerinde; bilgisayar üzerindeki kaynakların izinsiz bir şekilde kullanılmasına imkan sağlayan çeşitli açıklıklar bulunabilmektedir.Bu açıklıklar kötü niyetli kullanıcılar tarafından istismar edilerekuzakta olan bir bilgisayarın kontrolü ele geçirilebilmekte, bilgisayar üzerinde bulunan tüm veri kopyalanıp, silinebilmektedir. Silinmiş verilerin adli bilişimde kullanılan çeşitli yöntemlerle geri getirilebileceği Güllüce ve Benzer tarafından yapılan bir çalışmada açıklanmaktadır (Güllüce ve Benzer: 2015).

Teknolojideki gelişmelere paralel olarak; tehdit, zafiyet ve riskler de aynı hızda artmaktadır.Günümüzde kendi başına çalışan sistemlerden çok internet aracılığıyla entegre olarak çalışan ve bilgi paylaşımının yapıldığı sistemler daha ön plandadır.İnternete bağlı milyarlarca cihaz belirli protokoller kullanarak birbirleriyle haberleşmekte, bu sayede bilgi alışverişi yapabilmektedir.Bu cihazlardakigüvenlik açıklıkları bilgi sistemlerinin istismar edilmesine neden

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

olmaktadır.Bir bilgisayar yazılımının ya da donanımının istismar edilebilmesi için o istismara imkan sağlayan açıklığı üzerinde barındırması gerekmektedir.Siber korsanlar, istismar eylemine başlamadan önce hedef sistem üzerinde açıklık keşfi yapmaktadırlar.Açıklıktespitisonrasındabu açıklığı kullanabilecek istismar(exploit) yazılımı geliştirilmekte ya da üçüncü parti istismar araçları vasıtasıylamevcut açıklık istismar edilerek siber saldırılar gerçekleştirilmektedir.

Siber korsanlar tarafından düzenlenen saldırıların temel noktasını, sıfırıncı gün açıklıkları denilen üretici firmalar tarafından dahi bilinmeyen ya da fark edilemeyen zafiyetlerin oluşturduğu bilinmektedir.Symantec firmasının 2016İnternet Güvenliği Tehdit Raporunda; 2015 yılında bulunan sıfırıncı gün açıklıklarında %125'lik bir artış olduğu görülmektedir(Symantec, 2016). Sıfırıncı gün açıklıklarının yanı sıra, kamu oyuna yayımlanmış açıklıkların yamalarının yapılmaması ve istismar edilmesi nedeniyle de siber saldırılar gerçekleştirilmektedir. Açıklıkların saldırganlardan önce tespit edilip, kapatılmasıyla, istismarın engellenebileceği(TSE, 2015) değerlendirilmektedir.

İnternet bankacılığı uygulamasından kaynaklanan bir açıklık sadece bir kişinin ya da kurumun hesaplarında finansal bir kayba neden olurken, internet sunucusunda var olan bir açıklığın kapatılmaması sonucunda kuruma ait bir veritabanı çalınabilmekte ya da ülkenin kritik altyapılarına yapılan bir saldırı sonucunda tüm ülkede enerji kesintisi yaşanabilmektedir. Nitekim; 23 Kasım 2015 tarihinde siber saldırılar sonucu Ukrayna'nın üç bölgesinde elektrik kesintisiyaşandığı(CyberMag, 2016), saldırının sebebinin henüz tespit edilemediği, uzmanlar tarafından bunun gelişmiş bir siber saldırı olduğu yönünde görüş birliğine varıldığı(CipAlert, 2016) bildirilmiştir.

Bilgi sistem yöneticileri tarafından envanterde bulunan donanım ve yazılımların sahip olduğu açıklıkların belirlenmesine ve bunların kapatılmasına ihtiyaç duyulmaktadır.Riskleri düşürmek için var olangüvenlik açıklıkları'nın önceliklendirilmesi gerekmektedir.Ancak, bu açıklıkların sayısı çok fazla olduğunda ve her biri farklı ölçekler kullanılarak değerlendirildiklerinde, bilgi sistem yöneticileri bu devasa bilgiyi faydalı bilgiye dönüştürmektebir takım sorunlarla karşı karşıya kalmaktadır.OrtakGüvenlik Açığı Puanlama Sistemi (Common Vulnerability Scoring System [CVSS]) bu sorunu aydınlatmak için ortak bir çerçeve sunmaktadır.Bu sistemleaçıklık puanlaması standartlaştırılarak, açıklıklardan dolayı oluşabilecek risklerönceliklendirilebilmektedir(FIRST, 2015).

Bilişim cihazlarının ülke savunma sistemlerinde çok aktif şekilde kullanılmasıyla birlikte harekat ortamı genişlemiş, önceleri kara, deniz, hava ve uzay gücüyle sınırlandırılmışharekat ortamına asimetrik bir unsur olarak siber alan da eklenmiştir. Günümüzde "siber alan" harekatın beşinci boyutunu oluşturmakla birlikte klasik anlamdaki sınırlardan ve coğrafi konumdan bağımsız bir konumdadır.Ülkeler, hasım ülkelerin savunma sistemlerini siber saldırılarla engelleyerek geleneksel savaş sistemleri ile düzenleyecekleri saldırıları kolaylaştırabilir ya da hedef ülke kritik altyapılarına düzenlenecek bir saldırı ile o ülkede kargaşa çıkartabilmektedir.Nitekim; Eylül 2007'de İsrail tarafından düzenlenen meyve bahçesi harekatı ve 2010 yılındaki Stuxnet zararlı yazılımı harekat alanında siber saldırıların kullanılabildiğini gösteren en önemli örnekler arasındadır. Bu tip saldırıları engellemenin en önemli adımlarından biri de sistemlerdeki güvenlik açıklıklarının kapatılmasıdır.

Adli bilişim açısından değerlendirildiğinde ise bir sistem üzerinde yaşanan güvenlik ihlali sebeplerinin tam olarak ortaya çıkarılması açısından sistem üzerinde olabilecek güvenlik açıklıklarının ve bu açıklıklardan kaynaklanabilecek etkilerin olayı araştıran uzman kişiler tarafından bilinmesi,sayısal delil inceleme ve bilirkişi raporu hazırlama safhasında önemli bir husus olarak karşımıza çıkmaktadır. Olaylar çoğu zaman yapay olarak oluşturulan ortamlarda yapılan test ve denemeler neticesinde açığa çıkarılabilmektedir. Bu incelemeler esnasında dikkat edilmesi gereken en önemli hususlardan birisi de incelenen olayda kullanılan aynı işletim sistemi ve yazılımların aynı sürümünün olması gerektiğidir (Durmaz, 2014:273).

2. Materyal ve Metod

Bu çalışmada,bilgisayarlarda en çok tercih edilen işletim sistemleri tespit edilerek, bu işletim sistemlerinin barındırdıkları açıklıklar dikkate alınarak güvenlik açısından analizi yapılmaktadır.Bilgisayarlarda en çok kullanılan işletim sistemlerine ilişkin istatistiki bilgiler dünyada kabul görmüş web sitesi (StatCounter) toplanmıştır. İstatistiki bilgiler sorgulanırken coğrafi konum

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

olarak Türkiye ve Dünya dikkate alınmıştır.Açıklıklara ait veriler ise NIST (National Institute of Standart and Technology) tarafından geliştirilen veritabanından elde edilmiştir.Toplanan veriler bir veritabanında toplanmış, kabul görmüş standartlara göre yapılan açıklık puanlaması işletim sistemlerinin kullanım oranları da dikkate alınarak analiz edilmiştir. Bu çalışmada nicel verilerin analizinden elde edilen sonuçlar ile işletim sistemlerinin güvenlik açısından değerlendirilmesinin yapılması hedeflenmektedir.

Bunun için aşağıda belirtilen adımlar izlenmiştir:

•Açıklık, sıfırıncı gün açıklığı, istismargibi kavramlar açıklanmıştır.Bunun yanı sıra, yakın geçmişte yaşanan siber güvenlik olaylarında güvenlik açıklıklarınınetkisi araştırılmıştır.Yapılan önceki çalışmalar incelenmiştir.

•FIRST tarafından yayımlanan ve tüm dünyada bir standart olarak kulanılan Ortak Güvenlik Açığı Puanlama Sistemi (Common Vulnerability Scoring System[CVSS]) incelenmiştir.

•Dünya'da ve Türkiye'de en çok tercih edilen işletim sistemleri, son bir yılın (Haziran 2015-Haziran 2016) verileri dikkate alınarak "Statcounter" sitesinden sorgulanarak tespit edilmiştir.

•ABD'nin Ulusal Açıklık Veritabanı (National Vulnerability Database [NVD])ile CVEDETAILS veri tabanında bulunan bu işletim sistemlerine ait açıklık verileri MS Access'de hazırlanan veritabanında depolanmıştır. Depolanan veriler ve CVSS'de belirlenen eşitlikler ışığında açıklıkların istismar edilebilirliği ve risk seviyesi hesaplanmıştır.

•İşletim sistemlerinin kullanım oranları da dikkate alınarak açıklıklara ait kapsamlı bir analiz çalışması yapılmıştır.

•Ülkemizde yoğun olarak kullanılan yazılımlar ile kendi üretimimiz olan uygulama yazılımları ve milli işletim sistemleri için de benzer bir modelin ortaya konarak hayata geçirilmesi tavsiye edilmektedir.

3. Temel Kavramlar ve Yakın Geçmişteki Siber Saldırılar

Bilgisayar üzerinde çalışan en temel programlardan birininişletim sistemi olduğu bilinmektedir.İşletim sistemi, bilgisayar üzerinde çalışan diğer programlar ve servisler için güvenlik altyapısı sağlamaktadır.Bu nedenle, işletim sistemlerinin güvenliğinin korunması tüm sistemin güvenliği açısından oldukça önemlidir.İşletim sistemi üzerindeki açıklıklara ve zayıflıklara karşı gereken önlemler alınmaz ise, sistem istismar edilmeye uygun hale gelmekte, bu durum büyük güvenlik zafiyetlerinin ve siber saldırıların oluşmasına yol açabilmektedir.Bu sebeple, işletim sistemlerinin üzerindeki güvenlikaçıklıklarının kapatılmasınınson derece önemli olduğu değerlendirilmektedir.

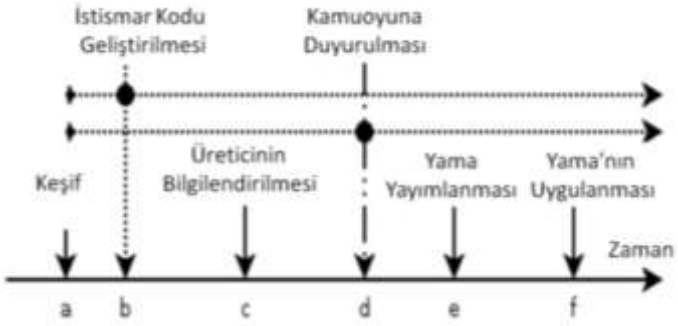
Ancak, bilgisayarlar üzerindeki güvenlik sorununungiderilmesi için sadece işletim sisteminde var olan açıklıkların kapatılması yeterli değildir.İşletim sistemlerinin üzerinde çalışan uygulama programlarındaki açıklıklar vasıtasıyla da işletim sistemi tarafından kullanılan kaynaklar istismar edilebilmekte ve hatta işletim sistemi ele geçirilebilmektedir.

Alınan güvenlik önlemlerininsaldırganlar tarafından aşılmasını sağlayan hata(Schultz, Brown ve Longstaff, 1990) olarak basit bir şekilde tanımlanan açıklık, Schneider tarafından; bir sistemin işletmesinde, uygulamasında ya da tasarımındaki bir hata yada zayıflık (Schneider, 1999:13), Amerikan Ulusal Altyapı Danışma Konseyi tarafından; bir bilgi sisteminin gizlilik, bütünlük ve erişilebilirliğinin üstü kapalı veya açık olarak ihlal edilmesine imkan sağlayan durumlar kümesi olarak tanımlanmaktadır(NIAC,2004).Shepherd ise; yazılımda bulunan bir kusurun; yetkisiz erişime, hakların yükseltilmesine ve hizmet dışı bırakmaya imkan sağlaması durumunda açıklık olarak nitelendirilebileceğini(Shepherd, 2003) belirtmektedir.Açıklıkların istismar edilebildiği; ancak, yazılım kusurlarında istismarın gerekli olmadığı(Weber, Karger ve Paradkar, 2005) yazılımdaki hata ile açıklık arasındaki temel fark olarak ortaya konulmuştur.Bu konuda otorite olarak kabul edilebilecek CVE konsorsiyumu ise açıklığı, bir sistem ya da ağa erişmek için siber korsanlarca "atlama taşı" olarak kullanılabilen yetenekler veya bilgiye erişme imkanı sağlayan yazılımdaki bir kusurvesistem yapılandırma problemi olarak tanımlanmaktadır (CVE, 2016).

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

Virüs, truva atı, solucan gibi zararlı yazılımlar çoğu zaman sistemde var olan açıklıkları kullanarak işlevlerini sürdürmekte ya da başka sistemlere bulaşmaktadırlar.Bunun en güzel örneği; Temmuz 2010'da fark edilen, İran'ın nükleer zenginleştirme programını hedef alan Stuxnet adlı zararlı yazılımdır. Şimdiye kadar en az 22 endüstriyel kontrol sistemine bulaştığı bilinen Stuxnet, Siemens PCS7, S7 PLC ve WinCC sistemlerinde, o güne kadar hiç görülmemiş dört sıfırıncı gün açıklığını ve yayılma yöntemlerini kullanan ileri düzey bir zararlıyazılımdır(Kara, 2011).

Açıklık keşfi tesadüfen olabildiği gibi, bu alanda profosyonel olarak çalışan kimseler tarafından da yapılabilmektedir.



Şekil 3.1. Açıklık Zaman Çizelgesi Modeli (Wright, 2014)

Şekil 3.1.'debulunan açıklık zaman çizelgesinde açıklığın a noktasında keşfedilmesinden sonra b noktasında bu açıklık için istismar kodunun geliştirildiği, c noktasında üretici firmanın bu konuda bilgilendirildiği, d noktasında açıklığın bir müddet sonra kamuoyu ile paylaşıldığı, e noktasında üretici firma tarafından açıklığın kapatılması için yama yayımlandığı ve f noktasında da yamanın ilgili yazılıma uygulanarak açıklıkların kapatılmaya çalışıldığı anlatılmaktadır. Burada b ve d noktasında belirtilen "istismar kodu geliştirme" ve "kamuoyuna duyurma" eylemlerinin sırasının değiştirilebileceği değerlendirilmektedir.

Farklı açıklıklar bilgisayar güvenliği üzerinde farklı etkilere sahiptirler.Açıklık puanlaması ile açıklığın potansiyel riskleri nicel olarak belirlenebilmektedir. Bu sayede güvenlik yöneticileri bir bilgisayarın yada ağdaki tüm bilgisayarların taşıdığı riskleri belirleyebilirler (Wang, Gao, Sun Q. ve Sun D.,2011).Açıklıkla ilgili yapılan araştırmalarda NVD, Exploit-DB, CVEDETAILSveritabanlarının kullanıldığı gözlemlenmiştir.

NIST(National Institute of Standards and Technology) ve MITRE tarafından başlatılan güvenlik ürün satıcıları konsorsiyumu ile sahada çalışanlar tarafından desteklenen ve gün geçtikçe dahada büyüyen NVD halen MITRE'nin sorumluluğunda işlevini devam ettirmektedir. Açıklıkları yayımlamak için kullanılan kapsamlı bir veritabanı olan NVD'nin, yazılım üreticileri tarafından onaylanmış ve yayımlanmış tüm CVE'leri kapsadığı(Allodi ve Massacci, 2012),CVE'lerin Ortak Güvenlik Açığı Puanlama Sistemi (Common Vulnerability Scoring System[CVSS]) ile puanlandığı bilinmektedir.CVE olmaksızın, güvenlik açıklıklarıyla ilgilenen her kurum ya da kruluşun aynı problemi farklı şekillerde tanımlayacağı öngörülmektedir.Açıklık paydaşları ile ortak dil konuşulması açısından CVE önemli bir standart haline geldiği bilinmektedir.CVSS, bilgi sistem açıklıklarının derecelendirilmesi için açık ve standart yöntem sağlamak maksadıyla tasarlanan bir açıklık puanlama sistemidir(Zhang, Caragea ve Ou, 2011).Bu sistemle açıklık puanlamasıstandartlaştırılarak, puanlama sonucundaaçıklıklardan dolayı oluşabilecek risklerönceliklendirilebilmektedir (FIRST, 2015).

Açıklıkların kapatılmasının önceliklendirilmesi sistem yöneticileri açısından önemli bir problemdir.Bu sorunun giderilmesinde, açıklıkların risk seviyesinin belirlenmesi en önemli hususların başında gelmektedir(Bozogri, Saul, Savage ve Voelker, 2010). CVSS puanlama sisteminde üç tip ölçüt grubu bulunmaktadır. Bunlar; Şekil 3.2.'de gösterilen Temel Ölçüt Grubu (Base Metric Group), Zamansal Ölçüt Grubu (Temporal Metric Group) ve Ortamsal Ölçüt Grubu (Environmental Metric Group)'dur. Her bir ölçüt grubu ayrı ayrı puanlanmakta 0 ile 10 arasında değişen bir değer almaktadır (NVD, 2016; Mell, Scarfone ve Romanosky, 2007; Ghani, Luna ve

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

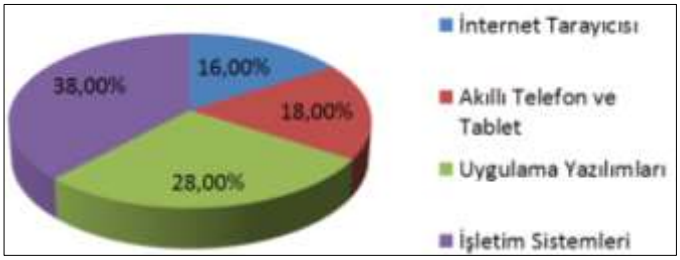
Suri, 2013). "0" ile "3,9" arası düşük, "4,0" ile "6,9" arası orta, "7,0" ile "10,0" arası ise yüksek şiddetli açıklık puanlarını ifade etmektedir (NVD, 2016; Ghani, Luna ve Suri, 2013).

Şekil 3.2.CVSS Ölçüt Grupları (Mell, Scarfone ve Romanosky, 2007)

*Temel Ölçüt Puanı = Yuvarla(((0,6*Etki)+(0,4*İstismar Edilebilirlik)-1,5)*f(Etki))*
Etki = 10,41(1-(1-CI)*(1-II)*(1-AI))*
İstismar Edilebilirlik= 20 AV*AC*AU*
Etki ==0 => f(Etki)=0, Etki !=0 => f(Etki)=1,176 (Mell, Scarfone ve Romanosky, 2007).
CI: Gizlilik Etkisi (Confidentialy Impact), II:Bütünlük (Integrity Impact),
AI:Erişilebilirlik (Availability Impact), AV: Erişim Vektörü (Access Vector),
AC: Erişim Karmaşıklığı (Access Complexity), AU: Kimlik Doğrulama (Authentication)
şeklinde ifade edilmektedir.

Genel itibarıyla, olumsuz ya da yanlış olan bir olayın meydana gelebilme olasılığı olarak ifade edilen risk, bilgi güvenliği bağlamında; iş veya personel bilgilerinin mevcudiyeti, gizlilik veya bütünlüğü etkileyebilen bir şey olarak karşımıza çıkmaktadır(Rao ve Nayak, 2014:79). Başka bir tanımda ise; sömürülen bir güvenlik açığının kullanıcının çalışma ortamında neden olduğu göreceli etki (Mell, Scarfone ve Romanosky, 2007) olarak bahsedilmektedir.Riskin önemine, ürünün; tehdit, zafiyet ve varlık değeri dikkate alınarak karar verilmektedir (Caballero, 2016). Bunun için;

Risk= Varlık x Tehdit x Zafiyet (Caballero, 2016)eşitliği ile risk hesaplaması yapılabileceğini dile getirmektedir.



Grafik 3.1. 2015 Yılında Keşfedilen Açıklıkların Dağılımı (Manes, 2016)

2014 yılında yapılan bir araştırmada, her gün ortalama 19 açıklığın NVD'na eklendiği, bu açıklıkların %80'in üzerinde bir oranla üçüncü parti uygulamalara ait olduğu, sadece %13'ünün işletim sistemlerine ve %4'ünün de donanımlara ait olduğu(Florian, 2015) açıklanmıştır. 2015 yılında yapılan benzer bir araştırmada ise her gün ortalama 25 açıklığın NVD'na eklendiği, bu açıklıların %28'inin uygulama yazılımlarına, %16'sının internet tarayıcılarına, %18'inin akıllı telefonlara ve %38'inin işletim sistemlerine ait olduğu belirtilmiştir(Manes, 2016). Ayrıca, 2015 yılında açıklık keşfedilen yazılımlar dikkate alındığında; en fazla açıklığın 430 açıklık ile OS X işletim sisteminde bulunduğu, ikinci sırada 387 açıklık ile iOS işletim sisteminin geldiği, üçüncü sırada ise 314 açıklık ile Adobe Flash Player uygulamasının yer aldığı görülmektedir(CVEDETAILS, 2016).İşletim sistemleri açısından değerlendirildiğinde; 2014 yılında %13 olan açıklık keşfedilme oranının, 2015 yılında %38'e çıkmış olması açıklık araştırmacılarının işletim sistemlerine yoğunlaştığını göstermektedir.

Bilinen açıklıkların dışında henüz keşfedilmemiş ya da keşfedilip kamuoyu ile paylaşılmamış açıklıklar da bulunmaktadır.Kişi, kurum ve organizasyonların sahip oldukları bilgi sistem varlıklarının zarar görmesine neden olan asıl konu, üreticinin, kullanıcının ve dolayısıyla kamuoyu tarafından bilinmeyen ve genellikle ancak saldırı sırasında haberdar olunan sıfırıncı gün "zero day"

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

güvenlik açıklıklarıdır (McQueen M.A., McQueen T.A., Boyer, ve Chaffin, 2009). Sıfırıncı gün açıklıkları, açıklığı keşfeden dışında başka bir kimsenin haberdar olmaması sebebiyle siber saldırı yapmada kullanılabilecek en etkili siber silah olarakkarşımıza çıkmaktadır.Açıklıkları kapatmaya yönelik yamalaraçıklığın kamuya duyurulmasından sonra yayımlandığı için güncel sistemler dahi henüz yayımlanmamış sıfırıncı gün açıklıklarının istismar edilmesi yoluyla ele geçirilebilmektedir (Garcia, Bessani, Gashi, Neves ve Obelheiro, 2013).

Bir açıklığı kullanmak üzere geliştirilen kod parçası(TSE,2015) olarak tanımlanan istismar(Exploit), Shepherd tarafından bir güvenlik açığından yararlanmak amacıyla geliştirilmiş bir araçya da komut dosyası olarak tasvir edilmektedir. Yetkisiz erişim kazanmak, kullanıcı haklarını yükseltmek veya hizmetin engellenmesi maksadıyla sistem üzerindeki bir açıklığın kullanılması, istismar etme olarak isimlendirilmiştir(Shepherd, 2003).İstismar, açıklıkların kullanılması suretiyle bilgisayarın ele geçirilmesi, üzerinde bulunan verilerin çalınması, silinmesi ya da bu verilere zarar verilmesi maksadıyla geliştirilen kod parçası şeklinde özetlenebilir.İstismar yazılımları vasıtasıyla siber saldırılar düzenlenebilmektedir.

Günümüzde ülkeler geleneksel savaş yöntemlerini kullanmadan taleplerini diğer bir ülkeye siber saldırılar ve kullandıkları siber silahlar vasıtasıyla kabul ettirebilmektedir. Gerçekleştirilen bu saldırılarda bir çok yöntem kullanılmıştır.Ancak, saldırı yapılacak sistemler üzerinde var olan kapatılmamış güvenlik açıklıkları ile kullanıcı zafiyetlerinin bu noktada saldırganların işini kolaylaştırdığı bilinmektedir.Geçmişte gerçekleştirilen siber saldırılar incelendiğinde bir çok saldırıda güvenlik açıklıklarının saldırganlara uzaktan erişim ve kod çalıştırma imkanı sunduğu anlaşılmaktadır.Sistemlerdeki güvenlik açıklıklarının kullanılmasının yanında, kullanıcı hatalarının da saldırıların oluşmasında en önemli fakörlerden biri olduğu gözden kaçırılmamalıdır.Saldırganların kullandığı akıl almaz yöntemlerle en güvenli olduğu düşünülen sistemlere dahi sızılabilmektedir (Çifci, 2013:163).

Tablo 3.1.'de yakın geçmişte düzenlenen siber saldırılara ilişkin bazı bilgiler verilmektedir. Bu saldırıların ortak özelliklerinden birisi yazılımlarda bulunan açıklıklarının saldırılarda aktif olarak kullanılmasıdır.

Sr.No.	Olay Adı	Aktif Olduğu Tarih	Kullandığı Açıklıklar	Etkilenen Sistem
1	Kırmızı Kod	19 Temmuz 2001	CVE-2001-0500	Windows NT 4.0, Windows 2000
2	Kızıl Ekim	2007 yılından itibaren aktif	CVE-2009-3129,CVE-2010-3333, CVE-2012-0158,CVE-2011-3544	MS Excel, MS Word, Acrobat Reader
3	Meyve Bahçesi Harekâtı	6 Eylül 2007	Bilinmiyor	Bilinmiyor
4	Conficker	Ekim 2008	CVE-2008-4250	Windows İşletim Sistemi
5	Night Dragon	Kasım 2009	CVE-2010-2568	Windows İşletim Sistemi
6	Stuxnet	Haziran 2010	CVE-2010-2568,CVE-2010-2729, CVE-2008-4250,CVE-2010-2772	Windows İşletim Sistemi, Siemens Step7 PLC
7	Duqu	14 Ekim 2011	CVE-2011-3402	Windows İşletim Sistemi
8	Pegasus	10 Ağustos 2016	CVE-2016-4655,CVE-2016-4656, CVE-2016-4657	iOS

Tablo 3.1. Yakın Geçmişte Açıklıklar Kullanılarak Gerçekleştirilen Siber Saldırılar

Internet Information Servicesyazılımındaki bir açıklığı istismar eden, 19 Temmuz 2001 tarihinde ortaya çıkan, dünya çapında 359 bin yama yapılmamış sistem üzerinde 14 saatten kısa bir sürede hızla yayılan ve 2,6 milyar doların üzerinde zarara yol açan Kırmızı Kod adlı solucan (Moore, Shannon ve Brown, 2002), güncellemesi yapılmamış açıklıkların nelere neden olabileceğini gösteren güzel bir örnektir.

Kaspersky firması tarafından tespit edilen zararlı yazılım 2007 yılından beri aktif olduğu, siber casusluk maksadıyla oluşturulduğu ve terabayt seviyesinde verinin elde edilmesinde kullanıldığı değerlendirilmektedir(GREAT, 2013).

6 Eylül 2007'de Suriye topraklarındaki bir tesisin nükleer silah geliştirdiği iddiası ile İsrail savaş uçakları tarafından vurulması olayıdır (Clarke ve Knake, 2011:3-5).Meyve Bahçesi Harekâtı "Operation Orchard" ismi verilen operasyon, saldırıdan dönen İsrail uçaklarına ait iki adet yakıt tankının topraklarımızda bulunması üzerine Türkiye kamuoyunda gündeme gelmiştir (Çifci,

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

2013:166). Bu olay, siber alan'ıngeleneksel harekat ortamlarında asimetrik bir unsuru olarak etkili bir şekilde kullanılabileceğine dair en iyi örneklerden birisi olarak karşımıza çıkmaktadır.

İlk olarak Ekim 2008'de tespit edilen Conficker (Piscitello, 2010), "Downup, Downadup ve Kido" olarak da adlandırılmaktadır.2003 yılında ortaya çıkan Welchia olarak adlandırılan solucandan sonra, en çok bilgisayara bulaşan solucan olarak bilinmektedir (Çifci, 2013:168).Dünya çapında 10 milyondanfazla bilgisayara bulaştığı tahmin tahmin edilen solucanın, Windows işletim sistemi güncelleştirmeleri gibi önemli servisleri ve yüklü güvenlik yazılımlarını devre dışı bıraktığı, bilgisayarların güvenlik yazılımları indirebileceği sitelere erişimlerini engellediği bilinmektedir (Messmer, 2009).

Kasım 2009 başlayan, petrol, enerji ve petrokimya şirketlerini hedef alan sosyal mühendislik, hedef odaklı oltalama saldırısı ve Windows işletim sisteminin sahip olduğu açıklıkları kullanan saldırıya "Nihgt Dragon" adı verilmiştir (McAfee, 2011). Bu saldırının temel amacı verilerin çalınmasıdır (Çifci, 2013:176).

Dünyanın ilk siber silahı olarak nitelendirilen Stuxnet zararlı yazılımı ilk kez Haziran 2010'da Beyaz Rusya'da küçük bir firma olan VirusBlokAda tarafından tespit edilmiştir (Pamuk, 2010).Stuxnet'in en önemli yanlarından biri daha önce bilinmeyen güvenlik açıklarını kullanmasıdır (Wright, 2014).500 KB uzunluğunda bir solucan olan Stuxnet'in, ustaca düşünüldüğü ve üretildiği, saldırıyı üç aşamada gerçekleştirdiği, öncelikle Microsoft Windows işletim sistemi ile çalışan bilgisayar ve ağlara bulaşarak kendini kopyaladığı ve yayıldığı, sonrasında hedefinde bulunan ve birçok endüstriyel cihazların kontrolu için kullanılan Programlanabilir Mantıksal Denetleyici (Programmable Logic Controllers [PLC]) olarak adlandırılan Siemens Step7 yazılımına bulaştığı, son aşamada ise PLC yazılımını bozup kontrol edilmesi gereken cihazın da anormal davranmasına neden olduğu (Kushner, 2013), aktif olmak için belirli bir zamanı beklediği, veri çalma gibi bir amacının bulunmadığı, 15000 satır koddan oluştuğu(Langner,2011) bilinmektedir.

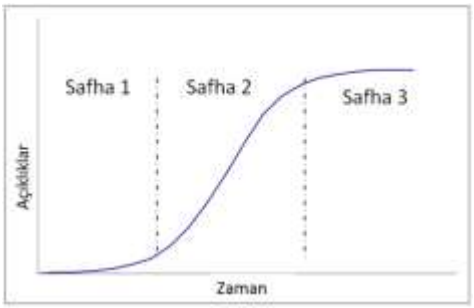
Stuxnet'e benzeyen, ancak tamamen farklı amaçlar için kullanılan, Windows işletim sisteminin sıfırıncı gün açıklığını kullanarak bulaşan ve yerleştiği bilgisayarda arka kapı açarak bilgisayardaki dosyaların çalınmasını sağlayan,Duqu, bir bilgisayar solucanıdır.E-posta'ya iliştirilen Microsoft Word dokümanı içine yerleştirilen ve Windows işletim sisteminde daha önce görülmeyen bir sıfırıncı gün açığını kullanan kod parçası ile bulaşmaktadır (Symantec Security Response, 2011).

10 Ağustos 2016'da İsrail merkezli NSO Group'un ürünü olan Pegasus adlı casus yazılım vasıtasıyla BAE'den (Birleşik Arap Emirlikleri) bir aktivistin telefonuna erişilmek istendiği, kurbanın gelen oltalama mesajındaki URL'e tıklamayarak bundan şüphelenmesinden ötürü erişilemediği, bu yazılımının Apple iOS işletim sisteminde var olan üç adet sıfırıncı gün açıklığını istismar etmek suretiyle casusluk faaliyetini yerine getirdiği(Paganini, 2016) açıklanmıştır.

4. Önceki Çalışmalar

Alhazmi ve Malaiya 2005 yılında yaptıkları çalışmada; Windows NT ve Windows 98 işletim sistemi açıklık verilerini, zaman aralıklarını dikkate alarak analiz etmişlerdir. Çalışmadatoplanan veriler ışığında işletim sistemlerinin tercih edilmesi üç safhaya ayrılmış ve açıklık tespiti bu safhalarla ilişkilendirilmiştir. Hedefteki işletim sistemi hakkında bilgi toplanan ve özelliklerinin anlaşıldığı safha1; "öğrenme safhası", işletim sisteminin daha çok kullanıcı tarafından kullanılmaya başlandığı, işletim sisteminin popülerlik kazandığı kullanıcıların bir süre daha mevcut işletim sistemini kullanmaya devam ettikleri safha2; "doğrusal safha" ve işletim sisteminin güvenlik yamalarının yayımlanma sıklığının azaldığı ve kullanıcıların da bu işletim sistemini yerine yeni çıkan işletim sistemlerini kullanmayı tercih ettikleri safha3; "doygunluk safhası" olarak adlandırılmıştır. Bu kapsamda oluşturulan Gayrete Dayalı (Effort Based) Model, işletim sisteminin yaygın kurulumu ve kullanımının, açıklık tespiti için sarfedilen çabaları aynı oranda arttıracağı varsayımı üzerine inşa edilmiştir(Alhazmi ve Malaiya, 2005).Yapılan çalışmada Şekil 4.1.'dekiüç safhalı açıklık-zaman S modeli ortaya konulmuştur. Şekil 4.1.'e bakıldığında en fazla açıklığın ikinci safhada keşfedildiği görülmektedir.

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128



Şekil 4.1.Üç Safhalı Açıklık-Zaman S Modeli (Alhazmi ve Malaiya, 2005)

Alhazmi, Malaiya ve Ray 2007 yılındaki çalışmasında; Windows işletim sisteminin 3 farklı sürümü ve Redhat Linux'un iki farklı sürümüne ait açıklık verilerini analiz edederek, açıklık yoğunlukları bakımından beş işletim sistemini kıyaslamaya tabi tutmuşlardır. Sonuçta, Windows XP'nin, Windows 95 ve Windows 98 sürümlerine göre ve Redhat Linux 7.1 sürümünün 6.2 sürümüne göre daha düşük yoğunlukta açıklık barındırdığı belirtilmiştir. Burada bahsedilen açıklık yoğunluğu, işletim sisteminde keşfedilen açıklık sayısının işletim sisteminin kaynak kodunun satır sayısına oranlanması sonucunda tespit edilmektedir.Kaynak kodu satır sayısı her bir 1000 satır için 1 birim olarak kabul edilmektedir. Sonuç olarak açıklık yoğunluğunun önemli ve faydalı bir ölçü birimi olduğu kanaatine varılmıştır (Alhazmi, Malaiya ve Ray, 2007).

Schryen'in 2009 yılında yaptığı çalışmada; sekiz farklı açık kaynak yazılım ile dokuz kapalı kaynak yazılımda var olan açıklıklarıdikkate almıştır. Güvenlik Açığı Açıklanması ArasındakiOrtalama Süre (Mean Time Between Vulnerability Disclosure[MTBVD]) adında bir teori ortaya koymuş, bu teoriye göre yazılımın ilk yayımlanmasından itibaren geçen gün sayısı bu zamana kadar yayımlanan açıklık sayısına bölünerek açıklık başına düşen gün sayısı tespit edilmiş, buna göre kapalı ve açık kaynak kodlu yazılımların açıklık kıyaslaması yapılmıştır. Bu rakam ilgili yazılım için ortalama açıklık tespit süresini de göstermektedir.Çalışmada ayrıca, yazılım satır sayısının da açıklık araştırmacıları için önemli bir faktör olduğu belirtilmiştir.İşletim sistemleri'nin ortalama CVSS puanı açısından kıyaslanmasında; en yüksek değerin 7,20 ile Windows 2000 ve Windows XP'ye ait olduğu, OSX işletim sisteminin 6,80 Red Hat Enterprise Linux ve Debian 3.1 sürümünün 4,90 ile üçüncü sırada yer aldığı görülmüştür(Schryen,2009).

Wang, Gao, Sun Q. ve Sun D. 2011 yılında yaptıkları çalışmada mevcut CVSS sistemini incelemişler, mevcut sistemin subjektif olan yönleri olduğunu düşünmüşler ve kendilerince daha gelişmiş bir yöntem önermişlerdir. Bu çalışmada ayrıca, açıklık puanlama sisteminin açıkları değerlendirmek ve onarmak için önemli bir puanlama sistemi olduğu, bu sayede güvenlik yöneticilerinin farklı açıklıkları esnek bir şekilde onarabildikleri, kendi geliştirdikleri Gelişmiş CVSS sistemi ile temel puanlamanın daha verimli ve daha doğru sonuçlar vereceğini ve açıklık değerlendirme işlemini basitleştireceğini belirtmişlerdir. (Wang, Gao, Sun Q. ve Sun D., 2011).

Allodi ve Massaci 2012'de yaptıkları çalışmada; NVD ve Exploit-DB'den açıklık araştırmalarında kullanılabilecek standart veritabanları olarak bahsetmişler, bu veritabanlarında yer alan puanlamanın gerçekte saldırıları temsil edip etmediğini analiz etmek için kendi veritabanlarını oluşturmuşlar, Symantec tarafından oluşturulan veritabanından 1000'den fazla açıklığı ve kara borsada kullanılan 103 açıklığı da dikkate alarak açıklıkların istismar edilebilirliği konusunda bir analiz çalışması yapmışlar(Allodi ve Massaci, 2012).

Marconato, Nicomette ve Kaaniche 2012 yılında yaptıkları çalışmada; OSVDB tarafından yayımlanan açıklık verilerinin karakteristiğini ele almışlardır.Bu çalışma, açıklığın keşfi, yayımlanması, açıklığa ilişkin güncelleme yayımlanması, ve istismar edilebilirliğine yoğunlaşmaktadır. Çalışmada, farklı işletim sistemlerinin (Windows, Unix ve Mobile) açıklıklarının gizlilik, bütünlük ve erişilebilirlik üzerindeki etkileri, açıklığın istismar edilebilirliği araştırılmıştır. Bu çalışmanın sonuçlarının sistem yöneticilerinin sahip oldukları sistemlerin risklerini analiz etmelerinde faydalı olacağı, mobil işletim sistemi açıklıkları için daha kısa sürede güncelleme yayımlandığı, Windows'un açıklığın açıklanmasını yama yayımlama tarihine yaklaştırmak için mümkün olduğunca geciktirdiği,

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

bunun da kullanıcıların açıklığın yayımlanmasından kaynaklı risklerin farkında olmamasına ve saldırganların da genellikle Windows açıklıklarını hedef almasından kaynaklandığı ileri sürülmüştür. Ayrıca, sıfırıncı gün açıklıklarının sistem üzerinde yüksek bir etkiye sahip olduğu belirtilmiştir (Marconato, Nicomette ve Kaaniche, 2012).

Garcia, Bessani ve diğerleri tarafından 2013 yılında yapılan çalışmada NVD'daki 11 farklı işletim sistemine ait açıklık verileri analiz edilmiştir. Bu açıklıkların birden fazla işletim sisteminde var olup olmadığı araştırılmıştır. 44000'den fazla açıklığın yayımlandığı NVD'dan OpenBSD, NetBSD, FreeBSD, OpenSolaris, Solaris, Debian, Ubuntu, Red Hat, Windows 2000, Windows 2003, Windows 2008 işletim sistemlerine ait 2563 tanesi seçilmiştir. Bu açıklıkların işletim sistemlerinin çekirdek, sürücü, sistem yazılımı ve uygulama yazılımı bileşenlerinden hangisine ait oldukları hususunda bir sınıflandırma yapılmıştır. Sonuçta işletim sistemleri üzerinde var olan açıklıkların %42,9'unun işletim sistemi üzerinde gelen uygulama yazılımlarından kaynaklandığı, %33,5'inin işletim sisteminin çekirdeği ile ilgili olduğu, %22,5'inin sistem yazılımlarından kaynaklandığı ve sadece %1'inin işletim sistemi ile donanım arasındaki irtibatı sağlayan sürücü yazılımlarından kaynaklandığı tespit edilmiştir. (Garcia, Bessani, Gashi, Neves ve Obelheiro, 2013).

Bozoklu, Çil ve Sağıroğlu tarafından 2013 yılında yapılan web tarayıcı açıklıklarının ele alındığı çalışmada; Internet Explorer, Google Chrome ve Mozilla Firefox'a ait açıklık değerleri NVD verileri dikkate alınarak incelenmiştir. Internet Explorer için 01.03.1997-10.07.2013 tarihleri arasında 1054 adet, Google Chrome için; 30.08.2008-10.07.2013 tarihleri arasında 877 adet, Mozilla Firefox için; 27.07.2004-26.06.2013 tarihleri arasında 1049 adet açıklığın paylaşıldığı tespit edilmiştir. Sonuç olarak; ülkemizde de NVD, OSVDB, Securityfocus ve Rapid7 gibi güvenlik açıklığı duyurusu yapan organizasyonların kurulması gerektiği, yazılımların ortak kriterler dikkate alınarak farklı seviyelerde test edilmesi gerektiği, yazılımların birer siber silah olduğu ve amaca uygun yazılımlarla ülkelere büyük çapta zarar verilebildiği, güvenlik açıklıklarının özellikle kritik alt yapılar dikkate alındığında hayati öneme haiz olduğu, açıklıkların saldırganlardan önce tespiti, kapatılması ve kamuoyuna duyurulmasının her geçen gün önemi artan ve yapılması gereken bir iş olarak karşımıza çıktığı, ülkemizde yazılım güvenliği ve güvenilirliğine ilişkin olarak üniversitelerde ar-ge çalışmalarına önem verilmesi gerektiği, yazılım zafiyetleri konusunda ülkemizde belirli standartların geliştirilmesi ve kritik görevlerde kullanılan yazılımların güvenlik testinden geçirilmesi gerektiği belirtilmiştir (Bozoklu, Çil ve Sağıroğlu, 2013).

Luo, Lo ve Qu tarafından 2014 yılında yapılan çalışmada; yazılım üreticileri tarafından kullanılan birçok açıklık puanlama sistemi bulunduğu ancak CVSS sisteminin açık tek sistem olduğu, diğer sistemlerin aksine CVSS'nin nicel bir ölçüm sistemi olarak tasarlandığı, bu sistemin eksik kalan bazı yönlerinin olduğu belirtilmiştir.2002 ile 2012 yılları arasında yayımlanan 54432 açıklığın NVD sisteminden indirildiği, CVSS puanlama sisteminde her bir açıklığın kendi içinde puanlandığı, CVSS puanlama sisteminin açıklığın neden olduğu sonuçları dikkate almadan sadece mevcut parametreleri dikkate alarak puanlama yapması sebebiyle neden olabileceği sonuçlar itibarıyle farklı karakteristikteki açıklıklar aynı puana sahip olabilmektedir. Bu sebeplerden ötürü kendileri yeni bir puanlama sistemi tasarlamışlar ve Yazılım Açıklık Puanlama Yaklaşımı (Software Vulnerability Rating Approach [SVRA]) olarak adlandırmışlardır.(Luo, Lo ve Qu, 2014).

Al-Zadjali tarafından 2015 yılında yapılan çalışmada; Android işletim sistemine ait açıklıkların analiz edilmesi hedeflenmiştir.Çalışmada, Android işletim sisteminin açık kaynak kodlu olması sebebiyle saldırganlar tarafından çekici bir platform olduğu vurgulanmış, Android işletim sistemi sürümlerinin tarihçesi oluşturulmuş, Android işletim sistemi mimarisinden bahsedilmiş, işletim sisteminin sahip olduğu açıklıklar yıllara ve açıklıközelliklerine göre analiz edilmiştir.Mevcut açıklıkların bu işletim sistemini kullanan kullanıcıları etkileyebileceği, Android işletim sistemini geliştirenler tarafından bu açıklıkların kapatılması gerektiği, siber korsanların bilgisayarların yanı sıra akıllı telefonlara da sızmaya çalıştıkları belirtilmektedir (Al-Zadjali, 2015).

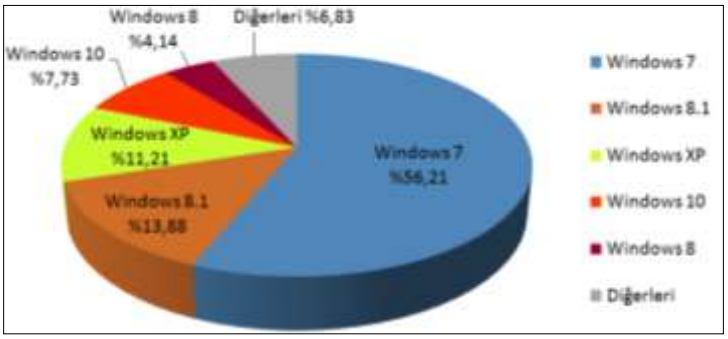
Edkrantz'ın 2015 yılındaki yüksek lisans tezinde; NVD ve İstismar Veritabanı (EDB) verileri kullanılarak makine öğrenmesi metoduyla bilinmeyen güvenlik açıklıklarının istismar edilebilme olasılığı ve zaman çerçevesi tahmin edilmeye çalışılmıştır. Çalışmada; veritabanından alınan veriler

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

ikili sınıflandırmaya tabi tutulduktan sonra 01.01.2010-31.12.2014 tarihleri arasındaki 7528 açıklık örnek olarak alınmış, çeşitli makine öğrenmesi algoritmaları ile istismar edilebilme olasılığı ve tahmini süreler hesaplanmaya çalışılmıştır (Edkrantz, 2015).

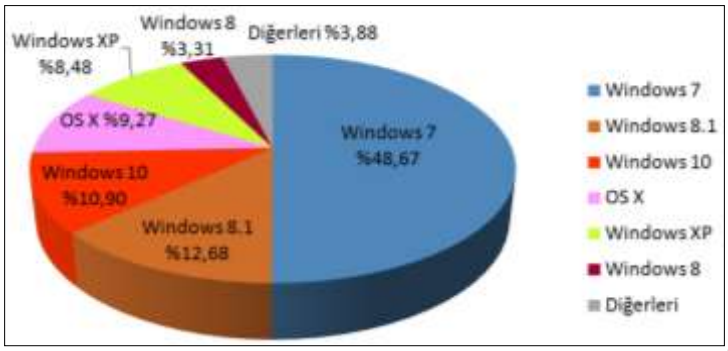
5. Bulgular

5.1. Türkiye ve Dünya'da Masaüstü ve Dizüstü Bilgisayarlarda En Çok Kullanılan İşletim Sistemleri



Grafik 5.1.1. Haziran 2015-Haziran 2016 Tarihleri Arasında Türkiye'de Masa Üstü ve Diz Üstü Bilgisayarlarda En Çok Kullanılan İşletim Sistemleri(StatCounter, 2016a)

StatCounter'dan alınan veriler ışığında; Haziran 2015-Haziran 2016 döneminde Türkiye'de dizüstü ve masaüstü bilgisayarlarda en çok kullanılan işletim sistemlerinin kullanım oranlarının yüzde olarak %56,21 ile Windows 7, %13,88 ile Windows 8.1, %11,21 ile Windows XP, %7,73 ile Windows 10, %4,14 ile Windows 8, ve %6,83 ile diğer işletim sistemleri olduğu Grafik 5.1.1.'de görülmektedir.Dünya genelinde iseaynı dönemde; %48,67 ile Windows 7'nin en çok kullanılan işletim sistemi olduğu dikkati çekmektedir. Hemen ardından %12,68 ile Windows 8.1, %10,90 ile Windows 10, %9,27 ile OS X, %8,48 ile Windows XP, %3,31 ile Windows 8 ve %3,92 ile diğer işletim sistemlerinin geldiği Grafik 5.1.2.'degörülmektedir.



Grafik 5.1.2. Haziran 2015-Haziran 2016 Tarihleri Arasında Dünya'da Masa Üstü ve Diz Üstü Bilgisayarlarda En Çok Kullanılan İşletim Sistemleri(StatCounter, 2016b)

Grafik 5.1.1.ve Grafik 5.1.2.'deki veriler dikkate alındığında; en çok kullanılan işletim sistemlerinin sırasıyla; Windows 7, Windows 8.1, Windows 10, OS X, Win XP, Windows 8 olduğu gözlemlenmektedir.

5.2. İşletim Sistemlerine Ait Güvenlik Açıklıklarının Analizi

Makalenin bu bölümünde işletim sistemlerinde bulunan açıklık verileri, açıklık yayını yapan birçok web sayfasına kaynak olan NVD veritabanından alınarak analiz edilmiştir.Açıklık veritabanı konusunda öncü olan NVD'nin bu alanda yayım yapan birçok web sayfasına ve organizasyona

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

kaynak olduğu gözlemlenmiştir.Bu çalışmada verilerini kullandığım "cvedetails.com" web sayfası da yayımladığı verilerin kaynağı olarak NVD'yi göstermektedir.

Toplanan veriler öncelikle bir veritabanına aktarılmıştır.Çalışmada, işletim sistemlerinin yayımlanma tarihinden itibaren 30 Haziran 2016 tarihine kadar yayımlanan 3497 adet açıklığa ait verilerbir araya getirilerek analiz edilmiştir. Bunun için, ilk olarak 30 Haziran 2016 tarihine kadaryayımlanan açıklıklara ilişkin veriler bir veritabanında toplanmış, CVSS puanlama sistemine göre Temel Ölçüt Grubu Puanı yeniden hesaplanarak toplanan veriler ile web sayfasında yayımlanan puanlar arasında tutarsızlık olup olmadığı araştırılmıştır.Sonrasında, toplanan veriler çeşitli kriterlere göre süzüldükten sonra analizler yapılmıştır.

Toplananveriler ışığında, bilgisayarlarda en çok kullanılan işletim sistemlerinden, yayımlanma tarihinden itibaren 30 Haziran 2016 tarihine kadar; Windows 10'un 125, Windows 8.1'in 266, Windows 8'in 254, Windows 7'nin 569, Windows XP'nin 727 ve OS X'in 1556 açıklığa sahip olduğu belirlenmiştir. Burada dikkat çeken bir husus OS X işletim sisteminin açıklık sayısı bakımından Windows işletim sistemlerine göre sayıca oldukça fazla olmasıdır. Bu durumun; Windows işletim sisteminin sürümleri itibarıyle sahip olduğu açıklıklar bakımından ayrı ayrı ele alınması, OS X işletim sisteminin ise piyasaya sürüldüğü 24 Mart 2001(Wikipedia, 2016) tarihinden itibaren tüm sürümlerinin sahip olduğu açıklılar bakımından kümülatif olarak birlikte sunulmasından kaynaklandığı değerlendirilmektedir.

Grafik 5.2.1. İşletim Sistemlerinin Yıllar Bazında Yayımlanan Açıklık Sayıları

Mevcut işletim sistemleri için en yoğun açıklığın 2015 yılı içerisinde yayımlandığı Tablo 5.2.1.ve Grafik 5.2.1.'deki veriler dikkate alındığında görülmektedir. 1997 ve 1999 yıllarında OS X işletim sistemi için yayımlanan açıklıkların işletim sisteminin önceki sürümlerinden kaynaklı olabileceği değerlendirilmektedir.2001 yılından itibaren OS X işletim sistemi için yayımlanan açıklıkların sayısında artış yaşanmış, 2006 ve 2007 yıllarında 106 açıklık yayımlanmış, 2008 yılından itibaren düşüşe geçerek 2013 yılından itibaren tekrar yükselmiştir. Windows 7 işletim sisteminde, açıklıkların sayısında 2011, 2013 ve 2015 yıllarında artış olduğu göze çarpmaktadır. Windows 8 ve Windows 8.1 için ise açıklık yayımlama durumunda 2015 yılında artış olduğu görülmektedir. En fazla açıklığın 2011 yılında yayımlandığı Windows XP işletim sistemi için bu tarihten sonra yayımlanan açıklık sayısının düştüğü, 2014 yılından sonra ise herhangi bir açıklık yayımlanmadığı dikkati çekmektedir.

Tablo5.2.1.'deişletim sistemlerinin yıllara göre açıklık miktarları yer almaktadır. İşletim sistemlerinin sürüm tarihleri ile açıklık miktarlarının artış ve azalış zamanları arasında ilişki kurulabileceği değerlendirilmektedir.Her yeni sürümde tespit edilen açıklık sayısında önce bir artış meydana geldiği zaman içerisinde ise yeni bir sürüm yayımlanmadığı sürece tespit edilen açıklık sayısında uzun dönemde azalma olduğu dikkati çekmektedir.Bulgular genel itibarıyla incelendiğinde; Alhazmi ve Malaiya tarafından ortaya konulan Üç Safhalı Açıklık-Zaman S Modeli'nin hemen hemen tüm işletim sistemleri için gerçekleştiği görülmektedir.

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

Açıklık Sayıları							
Yıllar	**OS X**	**Windows 10**	**Windows 7**	**Windows 8**	**Windows 8.1**	**Windows XP**	**Toplam**
1997	1						**1**
1999	1						**1**
2000						1	**1**
2001	5					10	**15**
2002	20					34	**54**
2003	25					22	**47**
2004	54					44	**98**
2005	96					66	**162**
2006	106					56	**162**
2007	106					34	**140**
2008	94					34	**128**
2009	81		15			88	**184**
2010	97		64			98	**259**
2011	74		102			101	**277**
2012	37		44	5		44	**130**
2013	71		100	58	7	88	**324**
2014	146		36	38	38	7	**265**
2015	417	53	147	146	151		**914**
2016	125	72	61	7	70		**335**
Toplam	**1556**	**125**	**569**	**254**	**266**	**727**	**3497**

Tablo 5.2.1. İşletim Sistemleri İçin Yayımlanan Açıklıkların Yılllara Göre Sayıları

Schryen tarafından 2009 yılında yapılan çalışmada tanımlanan Güvenlik Açığı Açıklanması Arasındaki Ortalama Süre eşitliğinden yararlanılarak oluşturulan Tablo 5.2.2.'dekiveriler dikkate alındığında; Windows 10 işletim sistemi için 2,576 ile en sık açıklık yayımlanan işletim sistemi olduğu, OS X'in 3,577 ile ikinci sırada olduğu, Windows 8.1'in 3,654 ile üçüncü, Windows 7'nin 4,267 ile dördüncü, Windows 8'in 4,622 ile beşinci, Windows XP'in ise 6,405 ile altıncı sırada olduğu görülmektedir.

İşletim Sistemi	İşletim Sistemi Yayım Tarihi	En Son Açıklık Yayım Tarihi	Aradaki Fark (Gün)	Açıklık Sayısı	Ortalama Açıklık Yayım Süresi (Gün)-G
Windows 10	29.07.2015	15.06.2016	322	125	2,576
OS X	24.03.2001	19.06.2016	5566	1556	3,577
Windows 8.1	17.10.2013	15.06.2016	972	266	3,654
Windows 7	22.10.2009	15.06.2016	2428	569	4,267
Windows 8	26.10.2012	13.01.2016	1174	254	4,622
Windows XP	25.10.2001	26.07.2014	4657	727	6,405

Tablo 5.2.2. İşletim Sistemlerinin Ortalama Açıklık Yayım Süresi

İşletim sistemlerinin sahip olduğu açıklıkların CVSS Temel ölçüt grubu puanı ortalama değeri dikkate alındığında Windows XP'nin 7,271 ile en yüksek değere sahip olduğu, Windows 7'nin 7,252 ile ikinci sırada geldiği, Windows 10'un 7,086 ile üçüncü sırada olduğu, Windows 8'in 6,964, Windows 8,1'in 6,816 ve OS X'in ise 6,403 değerine sahip olduğu gözlemlenmektedir. OS X işletim sistemi açıklık miktarı olarak fazla olsa da söz konusu puandikkate alındığında en düşük değere sahip olduğu görülmektedir.Tablo 5.2.3.'da işletim sistemine ait tüm açıklıklar dikkate alındığında bu sonuç değerlerine ulaşılmıştır. Risk faktörü hesaplanırken açıklıkların kapatılmasından sonra bu açıklığa ait CVSS Temel ölçüt grubu puan değerinin dikkate alınmaması gerektiği değerlendirilmektedir. Böylece Tablo 5.2.3.'da verilen tüm açıklıklara hiçbir yama ve güncellemenin yapılmadığı işletim sistemlerinin sahip oldukları CVSS Temel ölçüt grubu puanı ortalama değeri değişecektir.

İşletim Sistemi	CVSS Temel Ölçüt Grubu Puan Ortalaması-Z	Temsili Kullanım Oranı-KO	Ortalama Açıklık Yayım Süresi (Gün)-G	Hesaplanan Risk= Z*KO/G
Windows 7	7,252	0,5621	4,267	0,955
Windows 8.1	6,816	0,1388	3,654	0,258
Windows 10	7,086	0,0773	2,576	0,212
OS X	6,403	0,0927	3,577	0,165
Windows XP	7,271	0,1121	6,405	0,127
Windows 8	6,964	0,0414	4,622	0,062

Tablo 5.2.3.İşletim Sistemlerinin Ortalama CVSS Temel Ölçüt Grubu Puanı İle Hesaplanan Risk

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

Risk hesaplamasının; *Risk= Varlık x Tehdit x Zafiyet* (Caballero, 2016) eşitliği ile yapılabileceği belirtilmektedir. Burada, işletim sistemlerinin kullanım oranları(KO) varlık miktarı olarak alınabileceği, zafiyet yerine de ortalama CVSS Temel ölçüt grubu puanı'nınkullanılabileceği değerlendirilmektedir. Bunun yanı sıra, işletim sisteminin kullanım süresine bağlı olarak zaman içinde açıklık yayımlama miktarının düşeceği ve yayımlanan açıklıklara ait üretici firma tarafından yayımlanan yamaların yükleneceği göz önüne alınarak işletim sisteminin ortalama açıklık yayımlama süresi'nin de risk değerlendirmesinde dikkate alınabileceğidüşünülmektedir.Böylece, risk değerininişletim sistemlerinin; kullanım oranları, ortalama CVSS Temel ölçüt grubu puanı ve ortalama açıklık yayımlama süresi verileri dikkate alınarak hesaplanmasıylailgili bir öneri getirilmiştir.Buna göre;

Risk= Kullanım Oranı(KO) x Ortalama CVSS Temel Ölçüt Grubu Puanı(Z) / Ortalama Açıklık Yayım Süresi(G)

olarak önerilmektedir.Tablo 5.2.3.'te işletim sistemlerinin Türkiye ve Dünya'daki temsili kulanım oranları için hesaplanan değerler bir işletmedeki varlık miktarları dikkate alınarak hesaplanabilir. Tablo 5.2.3.'te hesaplanan risk değerleri dikkate alındığında; Windows 7'nin 0,955 ile ilk sırada yer aldığı, Windows 8.1'in 0,258ile ikinci sırada bulunduğu, Windows 10'un 0,212 ile üçüncü sırada, OS X'in 0,165, Windows XP'nin ise 0,127olduğu, Windows 8'in ise 0,062 ile son sırada yer aldığı görülmektedir. Ortalama açıklık yayım süresi uzadıkça o işletim sistemine ait risklerinde azalacağı,risk değerinin ve açıklık keşfinin kullanım oranıyla doğrudan ilişkiliolduğu değerlendirilektedir.

İşletim Sistemi	Düşük(0-3,9)	Orta (4,0-6,9)	Yüksek (7,0-10)	Toplam
OS X	150 (%9,64)	798 (%51,29)	608 (%39,07)	1556
Windows 10	13 (%10,40)	22 (%17,60)	90 (%72,00)	125
Windows 8.1	34 (%12,78)	62 (%23,30)	170 (%63,90)	266
Windows 8	25 (%9,84)	62 (%24,40)	167 (%65,94)	254
Windows 7	26 (%4,50)	132(%23,19)	411 (%72,23)	569
Windows XP	29 (%3,98)	191 (%26,27)	507 (%69,73)	727
Toplam	**277**	**1267**	**1953**	**3497**

Tablo 5.2.4. İşletim Sistemlerinin CVSS Temel Puanlarının Şiddet Seviyesine Göre Sayısı

Tablo 5.2.4. dikkate alındığında işletim sistemlerinin yüksek seviyeli(>=7) CVSS Temel Puanlarına bakıldığında Windows 7'nin %72,23'ü, Windows 10'un %72'si, Windows XP'nin %69,73'ü, Windows 8'in %65,94'ü, Windows 8.1'in %63,90'ı, OS X'in %39,07'sinin yüksek CVSS Temel Puanına sahip olduğu, orta seviyeli CVSS Temel Puanlarında ise OS X işletim sisteminin %51,29 ile en fazla orta seviyede açıklığa sahip olduğu görülmektedir.CVSS Temel Puan Değeri 10 olan açıklıklar dikkate alındığıda;124 adet ile en fazla OS X işletim sisteminde var olduğu görülse de, tüm OS X sürümleri dikkate alındığında bu rakkamın yaklaşık ortalama 12,4 olduğu varsayılabilir. CVSS Temel Puan değeri 10 olan açıklıkları en fazla barındıran işletim sistemi'nin 50 ile Windows XP olduğu , ardından da 21 ile Windows 7'nin geldiği, 12,4 ortalama değeri ile OS X'in üçüncü sırada yer aldığı, 8 ile Windows 8'in dördüncü sırada olduğu görülmektedir.

İstismar Edilebilirlik= 20 AV*AC*AU(Mell, Scarfone ve Romanosky, 2007)*

İşletim sistemlerinin sahip olduğu açıklıkların Ortalama İstismar Edilebilirlik Puanı dikkate alındığında; OS X'in 7,469 ile en yüksek değere sahip olduğu, Windows XP'nin 6,923 ile ikinci sırada geldiği, Windows 8'in 6,16 ile üçüncü sırada olduğu, Windows 8.1'in 6,104, Windows 7'nin 6,085 ve Windows 10'un ise 5,757 değerine sahip olduğu gözlemlenmektedir. Mevcut açıklıkların kapatılması için üretici firma tarafından yayımlanan güncellemeler yüklenmediğinde bu riskten söz etmek mümkündür.

6. Sonuç ve Öneriler

Gelişen teknolojik cihazlarda var olan donanım ve yazılım bileşenleri ile siber alan sınırlarının hızla genişlediği günümüzde, bireyler ve kurumlar tarafından alınan güvenlik önlemlerine ve geliştirilen yeni donanım ve yazılım çözümlerine rağmen siber ortamdaki saldırı sayısının her geçen gün daha da çok arttığı gözlemlenmektedir. Geliştirilen yazılımların satır sayısı arttığında açıklıkların

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

ortaya çıkma ihtimali de artmaktadır.Bilgi güvenliğinin temel bileşeni olan; gizlilik, bütünlük ve erişilebilirliği hedef alan bu saldırılar maddi ve manevi zararlara neden olmaktadır. Bu zararları tamamen yok etmek mümkün olmasa da, önceden ve yerinde alınacak uygun güvenlik tedbirleri ile zararın en aza indirilebileceği değerlendirilmektedir.İşte bu noktada hedefteki bilgi sistemi üzerinde var olan donanımsal ve yazılımsal açıklıkların kapatılması önemli rol oynamaktadır.Kapatılmayan her açıklık saldırıya uğrama riskini arttırmaktadır.

Açıklıkları kapatabilmek için öncelikle bu açıklıkların varlığından haberdar olunması, sonrasında bu açıklığın kapatılması için üretici firma tarafından yayımlanan yamaların uygun şekilde mevcut sisteme yüklenmesi ve bunun da kayıt altına alınması gerekmektedir.Bu açıklık yönetim sistemlerinin yamaların yüklenmesinden sorumlu yama yönetim uygulaması ile entegre bir şekilde çalışmasının var olan açıklıklara ait yamaların yüklenip yüklenmediği hakkında sistem yöneticilerine bilgi sağlayacağı, bu sayede açıklıkları kapatmak için daha az iş gücü sarf edileceği öngörülmektedir.

Bu çalışmada, Haziran 2015-Haziran 2016 döneminde bilgisayarlarda en çok kullanılan işletim sistemlerine ait 2016 yılının ilk yarısına kadar yayımlanan güvenlik açıklıklarının analizi nicel yöntemlerle yapılmıştır. Yapılan analizde; açıklık miktarı, ortalama CVSS Temel ölçüt grubu puanı, ortalama istismar edilebilirlik puanı ve bu çalışmada önerilen risk puanı dikkate alınmıştır.Ayrıca, çalışmada yapılan risk değerlendirmesinde işletim sistemlerinin kullanım oranları ve bu işletim sistemlerinin ortalama açıklık yayımlama süresi dikkate alınarak bir model ortaya konulmuştur.Bilgisayar üzerinde çalışan tüm programlara alt yapı sağlayan işletim sistemleri üzerinde güvenliğin sağlanmasının diğer tüm uygulamaların güvenliğinin sağlanmasından daha önemli olduğu, yapılan analizlerin bilgi sistem varlıklarını yöneten kişi ya da kurumlara, ellerinde bulundurdukları bilgi sistem varlıklarının güvenlik değerlendirmelerini yapmaları açısından fayda sağlayacağı değerlendirilmektedir.

Güvenlik açıklıklarından ve bunlarvasıtasıyla gerçekleştirilebilecek saldırılardan haberdar olmak, gerçekleşen bir siber olayın aydınlatılması esnasında bu olayın nasıl gerçekleştirilmiş olabileceğine ilişkin ip uçlarını elde etmemizi sağlayacaktır. Böylece gerçekleştirilen bir siber saldırının tüm güvenlik önlemlerinin alınmasına rağmen mi yoksa, alınmayan güvenlik önlemleri dolayısı ile mi gerçekleşip gerçekleşmediği hususunda olayı araştıran kişi ya da kişilerde kanaat oluşması sağlanacaktır. Bu durum adli bilişim açısından yazılım açıklıklarından haberdar olmanın önemini ortaya koymaktadır.Bunun yanı sıra bilirkişilerin olayları tam olarak aydınlatabilmeleri açısından yazılım açıklıkları ve bu açıklıkların nasıl istismar edilebileceği hususunda bilgi sahibi olması gerektiği değerlendirilmektedir.

Ülkemizde bu alanda yapılan akademik ve ticari araştırmalar incelendiğinde; yazılım açıklıkları ile ilgili yapılan çalışmaların çok düşük düzeyde olduğu gözlemlenmektedir.Ancak, son yıllarda TSE tarafından ulusal olarak kullanılan yazılımların açıklıklarının bir araya toplanmasına ilişkin bir veritabanı oluşturma çalışması başlatılmıştır.TSE tarafından başlatılan Açıklık Bildirim Programına tüm kamu kuruluşları ve özel sektör tarafından destek verilerek ulusal olarak kullandığımız yazılımlara ilişkin açıklıkların ve bu açıklıkların giderilmesi için yapılması gerekenlerle ilgili olarak veritabanı oluşturulması çalışmalarına destek verilmesi önerilmektedir.

Harekat alanına yeni bir boyut kazandırmasıyla; siber ortamdaki varlıkların ve bu varlıklara hükmeden insan gücünün harekata etkisi dikkate alınarak ülke savunmasında ve kritik altyapılarda kullanılan varlıklara ilişkin açıklık taramaları ve sızma testlerinin profosyonel ekiplerce düzenli bir şekilde yapılması, bu cihazlardaki açıklıkların kapatılması ve siber alanda görev yapan yetişmiş insan gücünün de kurumlar ve ülkeler tarafından en uygun şekilde değerlendirilmesi hayati derecede önemlidir.Ayrıca, bu alanda kullanılacak uygulama yazılımları ile işletim sistemi düzeyindeki yazılımların milli olarak geliştirilmesi ya da kullanılacak yazılımların kaynak kodları ile birlikte satın alınarak kaynak kodların güvenlik testlerinden geçirilmesi tavsiye edilmektedir.

Cihazlarda tüm güvenlik önlemlerinin eksiksiz alınmasına karşın, siber güvenlik bilincinden yoksun kullanıcı dolayısı ile saldırıya maruz kalınabilmektedir.Siber güvenlikteki en zayıf halkanın insan olduğu unutulmamalı, personelin farkındalığının arttırılması ve siber güvenlik bilincinin yükseltilmesi için kurum içi eğitimlerin sürekliliğinin sağlanması tesis edilmelidir.

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

Bundan sonraki çalışmalarda, mobil cihazlarda ve sunucularda kullanılan işletim sistemleri, internet tarayıcı programları ve kullanıcılar tarafından en çok kullanılan üçüncü parti yazılımlarınele alınabileceği değerlendirilmektedir.

Kaynaklar

Al-Zadjali, B., M. (2015, November). A Critical Evaluation of Vulnerabilities in Android OS: (Forensic Approach). *International Journal of Computer Applications*, 130(5), 0975-8887.

Alhazmi, O. H., and Malaiya, Y. K. (January, 2005). *Quantitative Vulnerability Assessment of Systems Software*. Paper presented at Annual Reliability and Maintainability Symposium, Virginia, USA.

Alhazmi, O. H., Malaiya, Y. K. and Ray, I. (2007).Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems.*Computers and Security*, 26(3), 219-228.

Allodi, L., and Massacci, F. (October, 2012). *A Preliminary Analysis of Vulnerability Scores for Attacks in Wild the EKITS and SYM Datasets*. Paper presented at Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security Conference, North Carolina, USA.

Ashton, K. That 'Internet of Things' Thing.*RFID Journal*. URL: http://www.rfidjournal.com/articles/view?4986, Son Erişim Tarihi: 02.10.2016.

Bozogri, M., Saul, L., K., Savage, S., and Voelker, G., M. (2010, 25-28 July). *Beyond Heuristics: Learning to Classify Vulnerabilities and Predict Exploits*. Paper presented at the Proceedings of the 16th SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'10), Washington DC, USA.

Bozoklu, O., Çil, C., Z., Sağıroğlu, Ş. (2013, 20-21 Eylül).*Yazılım Güvenlik Açıklıklarının Analizi İle Olası Zafiyet Öngörüsü*.6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansında Sunuldu, Ankara.

Brookshear, G. J. (2012). *Computer Science An Overview*(Eleventh Edition). New York: Pearson Addison-Wesley, 124.

Caballero, A. (2009). Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. John R. Vacca (Editor). *Computer and Information Security Handbook*.First Edition. Burlington, USA. Morgan Kaufmann Publishers.pp.231-232.

CipAlert.(Ocak, 2016).Ukrayna'daki Elektrik Kesintisinin Nedeni Koordineli Siber Saldırı.*CipAlert*.URL:http://www.cipalert.com/ukraynadaki-elektrik-kesintisinin-nedeni-koordineli-siber-saldiri/, Son Erişim Tarihi: 31.03.2016.

Clarke, R. E., and Knake, R. K. (2011). Siber Savaş, (Çev. Erduran, M.). İstanbul Kültür Üniversitesi Yayınları.(Eserin orijinali 2010'da yayımlandı), 48-51, 60.

CVE (Common Vulnerabilities and Exposures).(2016). Terminology.*Vulnerability*. URL: http://cve.mitre.org/about/terminology.html, Son Erişim Tarihi: 15.04.2016.

CVEDETAILS. (2016a). Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2015. *CVEDETAILS*. URL: http://www.cvedetails.com/top-50-products.php?year=2015, Son Erişim Tarihi:13.09.2016.

CyberMag.(2016). Ukrayna'daki Siber Saldırıdan Sonraki Elektrik Kesintisi 225.000 Müşteriyi Etkiledi.*CyberMag*. URL: http://www.cybermagonline.com/ukraynadaki-siber-saldiridan-sonraki-elektrik-kesintisi-225-000-musteriyi-etkiledi/, Son Erişim Tarihi: 31.03.2016.

Çifci, H. (2013). *Her Yönüyle Siber Savaş* (Birinci Baskı). Ankara: TUBİTAK Popüler Bilim Kitapları, 3-184.

Durmaz, Ş. (2014). Elektronik Verilerin Değerlendirilmesi. H. Çakır, M.S. Kılıç (Editörler). *Adli Bilişim ve Elektronik Deliller*. Birinci Baskı. Ankara. Seçkin Yayıncılık, s.273.

Edkrantz, M. (2015).*Predicting Exploit Likelihood for Cyber Vulnerabilities with Machine Learning*.Unpublished Master's Thesis, Chalmers Unıversıty of Technology Department of Computer Science and Engineering, Gothenburg, Sweden.

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

FIRST. (2015). Common Vulnerability Scoring System v3.0: Specification Document; *FIRST*, USA, 1-21.

Garcia, M., Bessani, A., Gashi, I., Neves, N., and Obelheiro, R. (2014).Analysis of Operating System Diversity for Intrusion Tolerance.*Software: Practice and Experience,* 44(6), 735-770.

Ghani, H., Luna, J., and Suri, N. (2013, 23-25 October).*Quantitative Assessment of Software Vulnerabilities Based on Economic-Driven Security Metrics*. Paper presented at the International Conference on Risks and Security of Internet and Systems, La Rochelle, France.

GREAT(Kaspersky Lab's Global Research & Analysis Team). (2013). The "Red October" Campaign–An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies. *Kaspersky*. URL: https://securelist.com/blog/incidents/57647/the-red-october-campaign/, Son Erişim Tarihi:03.05.2016.

Güllüce, Y. Z., Benzer, R. (2015). Hard disk failure and data recovery methods in computer forensic.*International Journal of Human Sciences*, 12(1), 206-225.

Kara, M. (2011). Zararlı Yazılımların Yeni Hedefi Hangi Kritik Altyapı Sistemleri Olacak?.*TUBİTAK BİLGEM Ulusal Bilgi Güvenliği Kapısı*. URL: http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/zararli-yazilimlarin-yeni-hedefi-hangi-kritik-altyapi-sistemleri-olacak.html, Son Erişim Tarihi: 30.03.2016.

Kushner, D. (2013). The Real Story of Stuxnet.*IEEE Spectrum*. URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, Son Erişim Tarihi: 30.03.2016.

Langner, R. (2011). Stuxnet decoder Ralph Langner speaks about Stuxnet. *Youtube*. 2011. URL: https://www.youtube.com/watch?v=n7UVyVSDSxY, Son Erişim Tarihi: 01.05.2016.

Luo, J., Lo, K., and Qu, H. (2014).A Software Vulnerability Rating Approach Based on the Vulnerability Database.*Journal of Applied Mathematics*, 2014(932397).

Manes, C. (2016). 2015's MVPs – The most vulnerable player. *GFI Lan Guard*. URL: http://www.gfi.com/blog/2015s-mvps-the-most-vulnerable-players/, Son Erişim Tarihi: 18.09.2016.

Marconato, G. V., Nicomette, V., and Kaaniche, M. (2012, October).*Security-Related Vulnerability Life Cycle Analysis*. Paper presented at the 7th International Conference on Risk and Security of Internet and Systems, Cork, Ireland.

McAfee. (2011). Global Energy Cyberattacks:"Night Dragon"; *McAfee White Paper*, California, USA, 3.

McQueen, M. A., McQueen, T. A., Boyer, W. F., and Chaffin, M. R. (2009, January).*Empirical Estimates and Observations of 0 Day Vulnerabilities*. Paper presented at the Hawaii International Conference on System Sciences, Hawaii.

Mell, P., Scarfone, K., Romanosky, S. (2007). A Complete Guide to the Common Vulnerability Scoring System Version 2.0; *FIRST*, USA, 1-23.

Messmer, E. (2009). Downadup/Conflicker worm: When will the next shoe fall?.*Network World*. URL: http://www.networkworld.com/article/2273085/lan-wan/downadup-conflicker-worm--when-will-the-next-shoe-fall-.html, Son Erişim Tarihi:03.05.2016.

Moore, D., Shannon, C., and Brown, J. (2002, November).*Code-Red: a case study on the spread and victims of an Internet worm*. Paper presented at the Internet Measurement Workshop, San Diego, USA.

NIAC. (2004). Vulnerability Disclosure Framework Final Report And Recommendations By The Council; NIAC, USA, 7-13.

National Vulnerablity Database (NVD). (2016). NVD Common Vulnerability Scoring System Support v2.*National Vulnerability Database*. URL: https://nvd.nist.gov/cvss.cfm, Son Erişim Tarihi: 10.06.2016.

Paganini, P. (2016). Apple fixed Zero-Day flaws exploited by nation-state spyware. *Cyber Defense Magazine*. URL: http://www.cyberdefensemagazine.com/apple-fixed-zero-day-flaws-exploited-by-nation-state-spyware/, Son Erişim Tarihi: 10.09.2016.

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

Pamuk, O. (2010). Stuxnet'i özel yapan ne?.*TUBİTAK BİLGEM Ulusal Bilgi Güvenliği Kapısı*. URL: http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/stuxneti-ozel-yapan-ne.html, Son Erişim Tarihi:30.04.2016.

Piscitello, D. (2010). Conficker Summary and Review.*ICANN*. URL: https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf, Son Erişim Tarihi:03.05.2016.

Rao, U. H., and Nayak, U. (2014). The infosec handbook an introduction to information security, New York: Apress Media, 79.

Schneider, F. B. (1999). (Editor).*Trust in Cyberspace*. Washington D.C.: National Academy Press, 13.

Schryen, G. (2009, 06-09 August). *Security of open source and closed source software: An empirical comparison of published vulnerabilities*. Paper presented at the Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS), San Francisco, California.

Schultz, E. E., Brown, D., S., and Longstaff, T. A. (1990).Responding to Computer Security Incidents; Guidelines for Incident Handling, *United States*, 55.

Shepherd, S. A. (2003). How do we define Responsible Disclosure?;*SANS Institute InfoSec Reading Room, SANS, USA,* 4.

StatCounter.(2016a). Global Stats.*Top 7 Desktop OSs in Turkey from June 2015 to June 2016*. URL: http://gs.statcounter.com/#desktop-os-TR-monthly-201506-201606-bar, Son Erişim Tarihi: 27.07.2016.

StatCounter.(2016b). Global Stats.*Top 7 Desktop OSs from June 2015 to June 2016*. URL: http://gs.statcounter.com/#desktop-os-ww-monthly-201506-201606-bar, Son Erişim Tarihi: 27.07.2016.

Symantec.(April, 2016).Internet Security Threat Report. Volume:21, 1-119. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_11125457&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2, Son Erişim Tarihi: 02.10.2016.

Symantec. (2016). Internet Security Threat Report; *Symantec, Volume:20*, California, USA, 1- 119.

TSE (Türk Standartları Enstitüsü). (2015). *TSE Açıklık Bildirim Programı*. Ankara:TSE, 1-7.

Wang, R., Gao, L., Sun, Q., and Sun, D. (2011, November). *An Improved CVSS-Based Vulnerability Scoring Mechanism*. Paper presented at the Third International Conference on Multimedia Information Networking and Security, Shanghai, China.

Weber, S., Karger, P.A., and Paradkar, A. (2005).*A Software Flaw Taxonomy:Aiming Tools at Security*. Paper presented at the Conference on Software Engineering for Secure Systems (SESS'05), Missouri, USA.

Wikipedia.(2016). OS X. *Wikipedia*. URL: https://en.wikipedia.org/wiki/Mac_OS-X_v10.0, Son Erişim Tarihi: 30.07.2016.

Zhang, S., Caragea, D., and Ou, X. (2011).*An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities*. Paper presented at the 22nd International Conference on Database and Expert Systems Applications (DEXA), Heidelberg, Germany.

Extended English Abstract

First computers, which had rather bulky and large structures and required punched cards to do any processing, while getting smaller in size after second half of the 20th century, became one of the essentials for the humanity as a device existing in every aspect of life with regards to their functions. With the internet use becoming widespread; every kind of action can be performed free of time and space with computers that provide great convenience at processing, saving and

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

forwarding information. With the widespread use of infrastructure presented by internet technology that enables data processing devices to communicate with each other, term of "cyberspace" has emerged. Along with simple actions like bill payment, complicated banking transactions, online shopping can easily be performed via computers. Along with this, it is known that computers are used actively in national defense systems with the purpose of preserving national security and operation of critical infrastructures.

Various softwares are required to administer and control these electronic devices that are used in almost every aspect of life. Because, it seems impossible for a regular user to have these devices that have no software on them and consisted only of electronic circuits, to perform any actions. One of the software we can label as the most important among these software, is operating systems. It is possible to describe operating system as a software that is between the user and computer hardware, making it possible to launch various application programs and responsible for controlling all processes in the computer system.

Operating systems provide security infrastructure to other programs and services that are running on the computer. Unless necessary precautions against vulnerabilities on the operating systems are taken, system becomes susceptible to exploitation, this situation gives attackers a ground to reach their goals. For this reason, fixing security flaws on operating systems is assessed as extremely important.

In parallel with technological advances; threats, vulnerabilities and risks increase at an equal rate. Today, systems that run integrated with each other via internet and share information are prominent compared to systems that work by themselves. Billions of devices connected to internet communicate with each other using certain protocols and can exchange information by this means. Security flaws on these devices give chance to exploitation of information systems and stealing, changing or destroying information.

In the center point of attacks performed by cyber pirates, are vulnerabilities called "zero-day vulnerabilities" which are unknown even to producing companies or undisguisable. Some security flaws still exist in software which undergo many test processes by software vendors that can not be noticed by even the suppliers. Discovering the vulnerabilities whose numbers are gradually increasing every day and taking necessary precautions to fix them have become a necessity. Giving common names to these vulnerabilities in order to speak the same language is very important. Studies regarding this subject, Common Vulnerabilities and Exposures (CVE), is started by MITRE organization in USA.

Common Vulnerability Scoring System (CVSS) provide a common framework to prioritize the risks that can be posed by these vulnerabilities. With this system, vulnerability scoring has been standardized.

Taking necessary precautions on operating systems running on computers that are very actively used for national security systems is vitally important for national security. Thusly, Operation Orchard carried out by Israel in 2007 and Stuxnet malware in 2010 revealed to the world how cyber-attacks can be used in the operation field. One of the most important steps to prevent this type of attacks is fixing all the software vulnerabilities used in national defense and critical infrastructure systems and regularly making penetration tests against these systems to discover and fix existing flaws before the attackers.

For specialists investigating the case, knowing possible security vulnerabilities and effects that may be caused by these flaws on the system from the aspect of completely enlightening the reasons for security breaches, is confronted as an important matter in the phases of examining electronic evidences and preparing expert reports in terms of computer forensics.

In this study, a new database is created by polling vulnerabilities in most widely used operating systems in Turkey and the World from USA National Vulnerability Database and CVEDETAILS databases. Regarding these vulnerabilities, scoring made by CVSS scoring system created by FIRST is examined, in the light of the results acquired by re-scoring vulnerabilities in said operating systems security analysis of the operation systems is done by quantitative methods. In the study also

Coşkun, A., &Bostancı, Ü. (2016). Bilgisayarlarda en çok tercih edilen işletim sistemlerinin güvenlik açıklıkları açısından değerlendirilmesi. *Journal of Human Sciences*, *13*(3), 4545-4564. doi:10.14687/jhs.v13i3.4128

studies in literature regarding this subject is examined, basic matters regarding the vulnerabilities are clarified and the role of vulnerabilities in exploitation of computers is explained. In the study information regarding recent cyber-attacks performed using vulnerabilities is also collected. Ultimately, when vulnerabilities contained by these systems is considered, analysis of the usability of operating systems from the aspect of security is aimed. As a result of analysis performed; it is evaluated that information system administrators can perform risk assessments regarding the information system entities they have. A model is produced considering the risk assessment performed in the study, usage rate of operating systems and average vulnerability disclosure time of these operating systems.

In recent years, it is recommended to support the endeavor of creating a database regarding the collection of vulnerabilities in the software that we use nationally by supporting the Vulnerability Notification Program started by TSE along with all public institutions and private sector. Furthermore, it is evaluated that using vulnerability management systems in institutions, performing penetration tests belonging to entities used in businesses and institutions by independent organizations is required. It is recommended to write a national operating system and using this system in public institutions and critical systems.

As a result of all precautions taken, it is not possible to absolutely ensure security. It should not be forgotten that the weakest link in cyber security is human, on the matter of increasing awareness of the personnel and enhancing cyber-security consciousness, ensuring continuity of education given to the user is recommended.