Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri

Hakan YAŞAR[a,*], Hüseyin ÇAKIR[b]

[a] *Adli Bilimler Bölümü, Fen Bilimleri Enstitüsü, Hacettepe Üniversitesi, Ankara, TÜRKİYE*
[b] *Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Eğitim Fakültesi, Gazi Üniversitesi, Ankara, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: hakanyasar80@gmail.com*

ÖZET

Günümüzde bilgi ve iletişim teknolojilerinde çeşitli uygulamaların artarak kişilerin günlük yaşantılarının vazgeçilmez bir parçası haline gelmesiyle birlikte gerek kamu gerekte özel sektörde birçok kurum hizmet sunumlarını siber ortamda gerçekleştirmektedir. Zaman ve coğrafi sınırlılıkların kalkarak anlık iletişim ve bilgi paylaşımının bulunduğu ve gerekli bilgi ve araçların kolaylıkla temin edilerek karmaşık ve organize saldırı ve tehditlerin gerçekleştirilebildiği bu ortamda etkin bir güvenlik anlayışı sadece ulusal ya da uluslararası alınabilecek güvenlik önlemleri ile sağlanamayacağı açıktır. Bu bağlamda siber ortamda ağırlıklı olarak saldırı ve tehditlere maruz kalan kurum ve şirketlerin kendi siber güvenliklerini sağlama adına gerekli adımları atmaları ihtiyaç olarak hissedilmektedir. Bu çalışmada giderek artan ve daha karmaşık hale gelen siber tehditlere karşı kurumsal bazda yapılabilecekler (genel bir çerçeve içinde) sunulmuştur. Ülkemizdeki kurumlara siber tehditlere karşı kurumsal siber güvenliklerini korumaları hususunda yardımcı olmanın amaçlandığı çalışma da görüşme ve doküman analizi gibi veri toplama yöntemleri kullanılmıştır. Çalışma sonucunda kurumsal siber güvenliğe yönelik tehditlerin etki ve zararlarını arttırırken kurumların siber güvenlik konusunda yeteri kadar farkındalık taşımadığının tespit edilmesinin yanı sıra verinin gizliliği, bütünlüğü ve erişebilirliğinin hedeflendiği kurumsal siber güvenliğin atılacak temel adımlar neticesinde etkili ve sağlam kılınarak yaşayan bir süreç olarak ele alınması gerektiği anlaşılmıştır.

Anahtar Kelimeler: *Kurumsal siber güvenlik, Siber tehdit, Siber güvenlik*

Institutional Cyber Security Related Threats and Measures

ABSTRACT

Increasing the range of applications in information and communication technologies, it has become indispensable part of people's daily life at the present time. As time and geographical limitations removed, instant communication and information sharing occurred and necessary information and tools easily provided, sophisticated and organized attacks and threats can be done. Therefore, it is clear that security measures which can be taken only by national or international will not ensure an effective understanding of security. It is important that necessary steps is taken for providing their cyber security since institutions and companies mainly exposed to cyber attacks and threats in cyber space. (within a general framework) it has been presented what it can be done against increased and more sophisticated cyber threats at corporate level in this study. Also, it has been aimed that it is assisted institutions in our country about institutional cyber related threats. İnterviews and

Geliş: 01/03/2015, Düzeltme: 20/04/2015, Kabul: 20/07/2015

document analysis were used as data collection methods. That impact and losses of institutional cyber security related threats increased and institutions do not have awareness enough about cyber security were determined at the end of the study. Moreover, It is understood that effective and robust institutional cyber security which targeted data confidentiality, integrity and accessibility need to be addressed as a living process at the end of the basic steps to be taken.

Keywords: *Institutional cyber security, Cyber threat, Cyber security*

I. GİRİŞ

Bilgi ve iletişim teknolojilerinde çeşitli uygulamaların artarak kişilerin günlük yaşantılarının vazgeçilmez bir parçası haline gelmesi, internet gibi zaman ve coğrafi sınırlılıkların kalkarak anlık iletişim ve bilgi paylaşımının bulunduğu ortamlarla birlikte siber güvenlik ile ilgili farklı bir ihtiyaç türü oluşmaya başlamıştır.

Günümüz siber ortamında saldırılara ağırlıklı olarak kurum ve şirketler maruz kalmaktadır. Kurum ve şirketlere yönelik bu saldırıların giderek artan bir çizgide ilerlemesine ve saldırı riskinin artmasına:

- Siber ortamda saldırı için gerekli yazılım ve bilginin ucuz ve kolay elde edilebilir olması,
- Dünyanın herhangi bir yerinden herhangi bir zamanda kişi veya sistemlerin kasıtlı ya da kasıtsız olarak bu saldırılara katılmalarının mümkün olması,
- Siber uzayın bütüncül ve kesintisiz iletişime açık yapısı nedeniyle kötücül yazılım ve benzeri tehditler ile yapılan saldırılar yoluyla sistemlerin birbirine zarar vermesi,
- Çok geniş kitlelere ulaşan kritik hizmet ve servislerin artarak bilişim sistemleri tarafından veriliyor olması,
- Birçok kurum ve şirketin kritik altyapılarının internete bağlı olması,
- İnternet kullanıcılarının çoğunun siber güvenlik bilincinin yetersiz olması,
- Saldırılara maruz kalma ihtimali olan kurum ve şirketler arasındaki işbirliği eksiklikleri,
- Kurumların genelde itibar ve pazar kaybı gibi nedenlerle kendilerine yapılan saldırıları gizlemesi,
- Kurumlarda bilgi güvenliği yönetiminin yeterli düzeyde olmaması,
- Kurumların üst düzey yöneticilerinin siber güvenlik hususunda yeteri kadar bilinçli olmamaları ve sahiplenmemeleri,
- Kurumların siber güvenlik konusunda yeterince iyi yapılandırılmış olmamaları ve güvenliğin sadece bilgi işlem birimlerinin sorumluluğu olarak görülmesi ve bu birimlerde çalışan personelin de yeterli seviye ve tecrübe de olmaması,
- Siber güvenliği ihlal eden olayların detaylı araştırılmasıyla ve oluşan suçun soruşturulmasıyla ilgili az sayıda yetkin personelin olması,
- Kurumların denetim süreçlerinde siber güvenliğe ilişkin denetimlerin yeterli seviyede olmayışı, donanım ve yazılım noktasında güvenlikli üretimin yetersizliği

gibi faktörler neden olmaktadır.

Siber korsanların geçmişe nazaran daha organize hale geldikleri günümüzde kurum ve şirketlere yapılan saldırı ve tehditler her geçen gün artarak devam etmekte ve daha karmaşık bir yapıya bürünmektedir. Buna karşın maalesef siber güvenlik kavramının (yapılan ulusal tatbikatlarda da ortaya çıktığı üzere) ülkemizdeki kurumlar tarafından yeterince ve doğru anlaşılamadığı görülmektedir.

ISC TURKEY 2012 sonuç bildirgesinde de belirtildiği gibi kurumların %61'inin kendilerini (özellikle web ortamından gelen) siber saldırıların hedefinde gördüğü (siber uzay diye tabir edilen sanal) ortamda kurumsal siber güvenliklerini sağlama zorunluluğu ortaya çıkmaktadır. Ayrıca eskiden sistemlere yapılan saldırılar daha çok sistemlerdeki bilgiye sızıp yeteneklerini göstermek isteyenlerin bireysel faaliyetleri iken artık belirli hedeflere daha organize ve karmaşık yapıda saldırılar düzenlenerek kurum ve şirketlere maddi zararlar verme ya da bu kurum ve şirketlerden elde ettikleri

bilgilerle kazanç sağlamaya yönelik ekonomik amaçlar güdülmektedir. Bu tür saldırılara maruz kalan kurum ve kuruluşların maddi yönden zarara uğramalarına kıyasla müşteri ve itibar kaybı gibi uğradıkları zararlar çok daha ciddi boyutta olmaktadır.

Gelişen ve karmaşıklaşan siber tehdit ve saldırılara en çok maruz kalan kurum ve şirketler olması sebebiyle kurumsal siber güvenlikle ilgili çalışmalara ihtiyaç duyulmasına rağmen siber güvenlikle ilgili yapılan çalışmaların (neredeyse tamamı) ulusal ve uluslararası boyutta olduğu görülmüştür.

Bu çalışmanın amacı, günümüzde kurum ve şirketlerin bilgi sistemlerini ve teknolojilerini (hizmet sunumlarını gerçekleştirdikleri artı bir değer olmaktan ziyade bir zorunluluk haline geldiği) siber ortamda kullanmaları neticesinde maruz kaldıkları (giderek daha sistemli ve karmaşık bir yapıya bürünen) siber tehditlere karşı kurumsal siber güvenliklerini sağlayabilmelerine yardımcı olmaktır. Bu amaç doğrultusunda siber güvenlik, siber güvenliğe yönelik tehditler ile bu tehditlerden korunma adına kurumsal bazda yapılabilecekler ele alınarak yanıtlar aranmıştır.

- Kurumsal siber güvenlikte temel amaç ve hedefler nelerdir?
- Kurumsal siber güvenliğe yönelik tehditler nelerdir?
- Siber tehditler ile bu tehditleri gerçekleştiren gruplar arasındaki ilişki nasıldır?
- Kurumsal siber güvenliği sağlama adına kurumsal bazda görülen eksiklikler ve yanlışlıklar nelerdir?
- Kurumsal siber güvenliğe yönelik tehdit ve saldırılara karşı kurumsal bazda yapılabilecekler nelerdir?

Bu çalışma ile siber tehditlerin etkilerinin artarak devam ettiği günümüzde kurumsal siber güvenlik kavramının net olarak anlaşılması, kurumsal siber güvenliğe yönelik tehditler hususunda farkındalık bilinci oluşturarak (veya arttırarak) bu tehditlere karşı etkin ve verimli mücadele yeteneği kazandırılması hedeflenmektedir.

Ulaşılmak istenen verilerin elde edilmesinin zorluğu ve uzman görüşlerine olan ihtiyaç nedeniyle görüşme ve doküman analizi gibi veri toplama yöntemleri kullanılarak araştırmacının kendisinin veri toplamada kilit rolde olduğu nitel araştırma yöntemlerinden yararlanılmıştır. Bu bağlamda kurumsal siber güvenlik ve kurumsal siber güvenliğe yönelik tehditlere ilişkin (doküman analizi kapsamında) siber güvenlik alanında yetkinliğe sahip ulusal ve uluslar arası kurum ve kuruluşların sunduğu raporlar ile yerli ve yabancı çalışmalar incelenmiş, bu tehdit ve saldırılara karşı kurumsal bazda yapılabileceklere ilişkin olarakta yaşları 25 ile 35 arasında değişen ve 2-7 yıl arasında değişen görev sürelerine sahip siber güvenlikle ilgili birimlerde çalışan 10 personel ile görüşülmüştür.

Günümüzde kurumsal siber güvenliğin yeni bir kavram olması ve (her ne kadar siber güvenlik alanında birçok araştırma yapılsa da) kurumsal bazda bu şekilde bir çalışmanın daha önceden yapılmamış olması nedeniyle, bu araştırmanın örnek bir çalışma olacağı ve sonraki araştırmalara kaynaklık ederek daha kapsamlı araştırmaların yapılmasına aracılık edeceği düşünülmektedir.

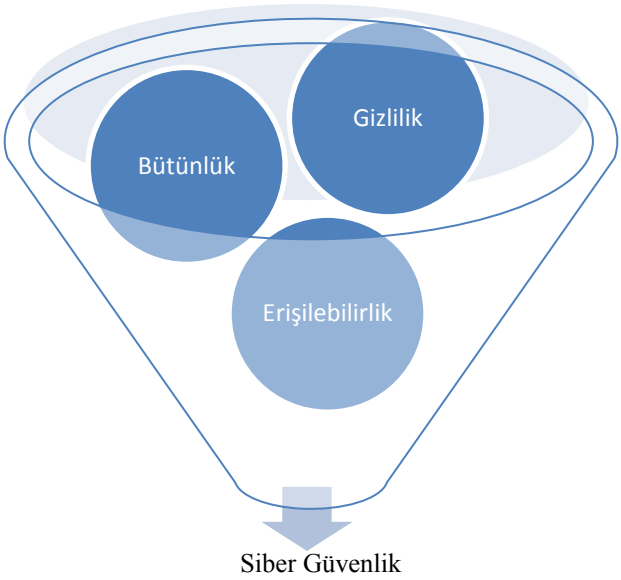
A. KURUMSAL SİBER GÜVENLİK

Siber güvenlik kavramı genel manada ulusal ve uluslararası bir ihtiyaç gibi düşünülse de bir toplumda bütünün güvenliği kurumların hatta birey bazında kullanıcıların güvenliğinin sağlanmasıyla daha kalıcı ve sağlam olacağı bir gerçektir. Yapılan birçok araştırma göstermektedir ki siber ortamda saldırılara maruz kalanlar ağırlıklı olarak kurum ve şirketlerdir.

Kurum ve şirketlerin türüne ve faaliyet gösterdiği alana göre bilgi güvenliği, bilgi teknolojileri güvenliği v.b. isimlerle ifade edilen kurumsal siber güvenlik, kurumsal bilgi güvenliği farkındalığının arttırılması, ülkenin siber uzayının güvenliğinin ve savunmasının arttırılması, kurumsal kritik bilgi ve iletişim sistem altyapılarının iş sürekliliğinin ve verilerin güvenliğinin sağlanmasını temin eder.

Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımları, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemleri ve siber ortamda iletilen ve/veya saklanan bilgilerinin tümünü kapsayan siber güvenlikte kritik altyapı ve bilgi varlıklarının tespit edilmesi ve bunların saldırılardan korunması maksadıyla öncelikli olarak güvenli risk analizlerinin yapılması gerekmektedir. Sonrasında kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin

siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulması ve idame edilmesinin amaçlandığı kurumsal siber güvenliğin temel hedefleri erişilebilirlik, bütünlük (aslına uygunluk ve inkâr edilemezliği de kapsar) ve gizliliktir[8]. *Gizlilik* ile verinin sadece yetkili kişilerce erişilebilir olması, *bütünlük* ile bilgi ve bilgi işleme yöntemleri ile veri içeriğinin değişmediğinin doğrulanabilmesi ve *erişilebilirlik* ile de erişime yetkisi olan kullanıcıların ihtiyaç duyduklarında bilgi ve ilişkili varlıklara erişebilmesi kastedilmektedir[6]. Kısaca kurumlar için siber güvenliğin amacı; verinin gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanması ve kritik bilgi ve iletişim alt yapılarında performans ve iş sürekliliğinin sağlanmasıdır.



Şekil 1. *Siber Güvenliğin Temel Hedefleri*

B. KURUMSAL SİBER GÜVENLİĞE YÖNELİK TEHDİTLER

Siber ortamda bulunan verinin gizliliği, bütünlüğü ve erişilebilirliğine yönelik istenmeyen durumlara yol açabilme yeteneği de denebilecek siber tehditler, siber ortamdaki güvenlik açıklıklarını kullanma potansiyeline de sahip olabilmektedirler. Kurumsal siber güvenliğe yönelik tehditler:

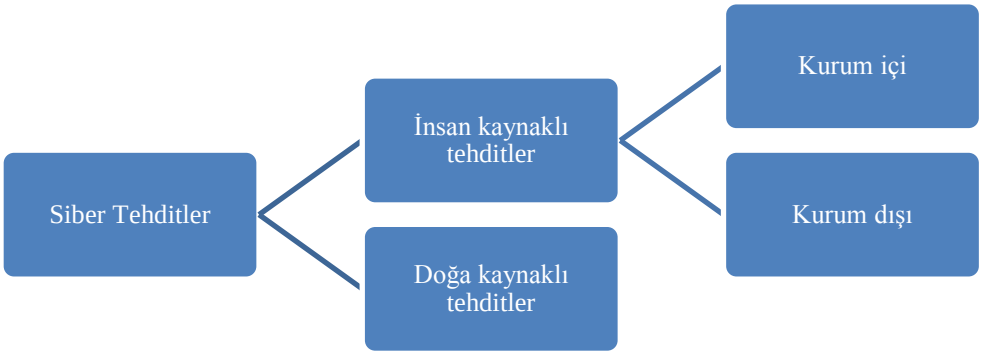
- İnsan kaynaklı tehditler:

(1) *Kurum içi*: Eğitimsiz ve bilinçsiz kullanıcılar, casuslar ve art niyetli personel davranışları, sistem yöneticisi hataları v.b…

(2) *Kurum dışı*: İnternet ortamından gelen tehditler ile yetkisiz ve izinsiz erişim, casusluk, hırsızlık v.b. faaliyetler…

- Doğa kaynaklı tehditler: Sel, yangın, deprem v.b…

Günümüzde kurum ve şirketlerin özellikle internet ortamından gelen siber tehditlere maruz kaldığı bilinmektedir. Bu bağlamda (ENISA' nın 250'nin üzerinde raporu inceleyerek elde etmiş olduğu veriler ışığında) son zamanların ve önümüzdeki dönemlerde de etkilerini sürdürecekleri tahmin edilen (özellikle kurumların web uygulamalarına yönelik) siber tehditler aşağıda maddeler halinde sayılarak kısaca açıklanmaktadır.



Şekil 2. *Siber tehditlerin sınıflandırılması*

B.1. İzinsiz İndirmeler (Drive by download)

Saldırganların belirledikleri bir siteye yerleştirdikleri (bunlar genelde ilerleyen sayfalarda tanımı verilecek olan exploit kitler denen) zararlı kodların siteyi ziyaret eden kullanıcıların sisteminin otomatik olarak taranıp bulunan güvenlik açıklıklarının kullanılmasıyla sisteme yüklenmesi şeklinde gerçekleşir. Özellikle saldırganlar tarafından mobil cihazların hedeflendiği izinsiz indirme yöntemi ile yapılan saldırılar genelde zararlı linklerin kullanıcılar tarafından tıklanmasıyla yapılmaktadır[20].

B.2. Kod Çalıştırma (Kod Enjeksiyonu)

Otomatik saldırı araçlarının artması bu tür tehditlerin görülme sıklığını da arttırmıştır. Saldırganlar tarafından bu tür araçlar kullanılarak (kısa bir süre içinde) güvenlik açığı taraması yapılabilmekte ve tespit edilen bu açıklıkları kullanacak zararlı kodlar oluşturularak hedef üzerinde çalıştırılması sağlanmaktadır. En çok bilinen kod çalıştırma (kod enjeksiyonu) yöntemleri:

- Çapraz site betik saldırısı (Cross site scripting attack- XSS)
- Siteler arası istek sahteciliği (*Cross-site request forgery-CSRF*)
- SQL enjeksiyonu
- Xpath Enjeksiyonu
- SSI enjeksiyonu
- İşletim sistemi enjeksiyonu
- LDAP enjeksiyonu
- Dizgi Formatı

B.3.Botnet

Saldırganlar tarafından internet kullanıcılarının sistemlerine yüklenen zararlı yazılımlar yoluyla (zombi de denen) *bot* adında birçok bilgisayarın oluşturduğu ağ sistemine *botnet* denmektedir. Saldırganlar oluşturdukları botnet sayesinde tek bir merkezden dünyanın farklı noktalarındaki bilgisayarları (istenmeyen e-postalar göndermek, virüs yaymak, sunucu ve sistemlere saldırmak v.b.) kendi amaçları doğrultusunda yönetebilmektedirler.

B.4. Kötücül Yazılımlar

Mobil cihazlar üzerindeki yayılımı diğer platformlara göre daha etkili olan kötücül yazılımlar sistem üzerindeki açıklıkları bularak hedeflenen veri ya da verileri elde etmek için kullanılmaktadır. Çalışma kapsamında araştırılan bazı kötücül yazılımlar şunlardır:

B.4.1. Truva atı (Trojan)

Bilgisayarın kontrolünü uzaktan ele geçirerek ekranın görüntüsünün alınması, uzaktan komutlar çalıştırılması ve dosyalar üzerinde izinsiz ve yetkisiz işlemler yapabilme gibi imkânlar veren truva atları (trojan) genelde e-posta, internet üzerinden oynanan popüler oyunlar, MSN gibi mesajlaşma programları ya da internet üzerinden yüklenen ücretsiz ve lisanssız yazılımlar yoluyla yayılmaktadırlar [5].

Solucanlardan farklı olarak:

- Sisteme bulaştığında hangi programla bulaşmışsa o programın açılmasını bekler (açılmadığı sürece aktifleşmez).
- Direkt olarak bilgisayarın işletim sistemine zarar verebilir.
- Bilgisayar üzerinde (monitör izleme, programlar açabilme v.b…) işlemler gerçekleştirerek tüm kontrolü ele alabilir [14].

B.4.2. Solucan (Worm)

1975 yılında John Brunner tarafından yazılan "Shockwave Rider" (Şok Dalgası Binicisi) adında bir bilim kurgu romanında, bir bilgisayar ağı üzerinden kendi kendini yayan bir programa verdiği isimden gelen solucanlar başka dosyaları değiştirmese de etkin bir biçimde bellekte durarak kendilerini kopyalayabilir ve (genelde) e-posta, FTP ve HTTP gibi yollarla kendilerini yayabilirler. Solucanlar çoğu kez (bir fotoğraf ya da metin dosyası içerecek şekildeki e-postaların içindeki) bir eklentinin kullanıcı tarafından çalıştırılarak kendini sisteme kopyalaması ve kopyalandıkları sistemdeki kullanıcıların adres defterinde bulunan her bir adrese bulaşmalarıyla yayılırlar. Bunun dışında (W32.Nimda.A@mm ve W32.Aliz.Worm gibi) internet üzerinde yaptığı taramalar sonunda açık kapıları olan veya güvenlik duvarı bulunmayan sistemlere bulaşarak yada yerel ağ üzerinde (ortak paylaşıma açılmış bir klasör şeklinde kendini göstermesiyle) kullanıcıların çalıştırması sonucunda da yayılabilmektedirler [12].

Virüslere benzer yapıda olan solucanların yayılmak için kendilerini çalışan bir programa iliştirmeye veya bir parçası olmaya ihtiyaçları bulunmamaktadır. Solucanlar ağdaki band genişliğini kullansa bile (ulaştıkları sistemdeki dosyaları değiştiren veya tahrip eden virüslere kıyasla) ağ için çok zararlı değildirler [17].

B.4.3. İstismar kodları (Exploit kit)

Hedef sistem üzerindeki açıklıkları tespit edip bu açıklıkları kullanarak sisteme yönelik saldırılar gerçekleştirebilen exploit kitler çok sayıda fonksiyon çeşitliliği, yapılandırma seçenekleri sunan kullanıma hazır yazılımlardır. İnternet kullanıcıları çoğunlukla zararlı URL'lere tıklamalarıyla exploitleri sistemlerine yüklerler. Exploit kitlerin anti virüs programları gibi yazılımlar tarafından tespit edilmemeleri için exploit geliştiriciler bu zararlı kodları şifrelemek için uğraşmaktadırlar [20].

Günümüzde en yaygın web tehdidi olarak görülen Blackhole exploit kiti bulaştığı sistemlerde kullanıcılar hakkında bilgiler toplayan izleme mekanizmaları içermektedir. Bu bilgiler içinde kurbanların ülkesi, işletim sistemleri, kullandıkları web tarayıcı ve kurbanların sistemlerindeki yazılımlardan istismar edilenler bilgisi bulunmaktadır [16].

B.4.4. Sahte antivirüs yazılımları

Bilgisayara zarar vermek amacıyla yazılan ancak (Javascript kodlarını kullanarak bilgisayardaki işletim sistemine göre uygun ara yüze sahip olabilme yetenekleri sayesinde[9]) kendilerini birer virüs koruma programı ya da casus yazılım engelleme aracı şeklinde gösterebilen yazılımlardır. Genelde bilgisayarınızda çok sayıda virüs tespit edildiği ve bunları temizlemek için (verilen linke tıklanarak) bir program indirmeniz gerektiğini belirten mesajlarla bulaşırlar. Başka bir yolda e-posta yoluyla sahte

anti virüs programının linki kullanıcıya gönderilerek (30 günlük ücretsiz kullanım hakkı olduğu gibi) ifadelerle kullanıcın bilgisayarına programı yüklemesi sağlanarak da bulaşabilmektedir.

Bazı sahte anti virüs yazılımların yapabilecekleri şu şekilde sıralanmaktadır [11]:

- Sizi bir dolandırıcılık işlemi için kandırma (örneğin, bir programın aslında bulunmayan ücretli sürümüne yükseltme).
- Kişisel bilgilerinizi çalmak için sosyal mühendislik kullanma.
- Verilerinizi çalarken saptanmayacak kötü amaçlı yazılımlar yükleme.
- Sahte veya aldatıcı uyarılar içeren pencereler açma.
- Bilgisayarınızı yavaşlatma veya dosyaları bozma.
- Windows veya geçerli virüsten koruma yazılımlarının güncelleştirmelerini devre dışı bırakma.
- Virüsten koruma satıcılarının web sitelerini ziyaret etmenizi önleme

B.5. Kimlik Hırsızlığı ve Oturum İhlali

Saldırganlar tarafından çıkar sağlama ya da dolandırıcılık gibi faaliyetlerde kullanmak üzere (parolalar, kullanıcı adları, bankacılık ve kredi kartı bilgileri v.b.) kurbanın kişisel verilerine erişme anlamındaki kimlik hırsızlığı (ve bunun neticesinde işlenen dolandırıcılık) tehditleri en başarılı uygulamaların gerçekleştirildiği tehditler olmanın yanında geniş çaplı zarar verme potansiyeline sahip birçok veriye erişilebilmesini de sağlamaktadır.

Trojan gibi kötücül yazılımlar sahip oldukları zararlı kodlar sayesinde kimlik hırsızlığı yapabilmektedirler. Örneğin 2013 yılında görülen (Zeus, Citadel v.b.) trojanlar, mobil cihazlara 2 faktörlü kimlik doğrulama saldırıları gerçekleştirme de kullanılmıştır. Bu tip çoklu saldırılar sonucunda erişilen verilere ilişkin büyük bir pazar oluşmuştur [20].

B.5.1. Sazan avlama (Phishing)

İngilizce Password Harvesting Fishing kelimelerinden türetilen Phishing (sazan avlama) yönteminde kullanıcıların şifre, kullanıcı adı, kredi kartı bilgileri v.b. bir takım bilgilerini elde etmek amacıyla (genellikle) e-postalar göndererek kullanıcının (çeşitli kandırmacalarla) e-posta içindeki linke tıklaması sağlanarak, önceden hazırlanmış sahte web sayfalarını ziyaret ettirilmesiyle (bu sayfalardaki ilgili alanları doldurmaları sağlanarak) bilgilerinin elde edilmesidir [5].

B.6. Spam

İnternette kullanıcıların herhangi bir talebi olmaksızın (çok yüksek sayıda kopyaları üretilen) genelde ticari reklam içerikli veya belli bir görüşün propagandası amacı ile oluşturulan e-postalar olarak bilinen spamlar, çabuk zengin olma kampanyaları veya güvenilmeyen ürünlerin duyurulması şeklindedir. Spam gönderme için genellikle kullanıcılarının adreslerinin güvenliğine yeterince önem vermeyen sitelere yapılan üyeliklerde, sitelerin forum ve ziyaretçi defterlerinde veya sisteme bulaşan virüsler vasıtasıyla elde edilen e-posta adresleri kullanılmaktadır [10].

Tüm e-posta trafiğinin %75'ini oluşturan spamlar zararlı kod içeren URL linklerin, kötücül yazılımların yayılması ve dolandırıcılıklar için bir kaynak durumundadır. Günümüzde spam üreticileri spam filtreleme yazılımlarının performanslarını düzenli olarak kontrol etmelerinin de etkisiyle spamlara karşı etkin bir korunma sağlanamamaktadır [24].

B.7. Veri İhlalleri ve Bilgi Sızıntısı

Bu tehditle kasıtlı ya da kasıtsız olarak bilginin açığa çıkmasıyla meydana gelen veri kayıpları kastedilmektedir.(Bilgi yönetim varlıklarındaki hatalarda olduğu gibi) Bu tehdit içsel ve dışsal

faktörlerden kaynaklanabilmektedir. Her iki durumda da iyi ya da kötü niyetli sebepler olabilir. Veri ihlalleri hem kötücül eylemlerin etkinliği hem de kurumsal bilgilerin korunma düzeylerinin önemli bir göstergesi olarak değerlendirilmektedir. Veri ihlalleriyle ilgili özellikle kurum içindeki personeller önemli bir rol oynamaktadır. Mevcut güvenlik tedbirlerinin etkinliği hususunda önemli bir gösterge olan (% 70 kadarı basit ve düşük seviyeli saldırılar olan) veri ihlallerini engellemek için basit ve düşük maliyetli güvenlik kontrolleri uygulanması yeterlidir. Bilgi sızıntısı ise, veri ihlalinden farklı olarak kurumların güvenlik sistemlerine ilişkin teknik bilgilerin açığa çıkarılmasına dayanır. Güvensiz dosya transferleri ve mobil cihazlardaki basit şifrelemeler bilgi sızıntısına yol açabilmektedir[20].

B.8. Fiziksel Zarar Verme ve Hırsızlık (Kayıp)

Yangın, sel, deprem v.b. doğa kaynaklı tehditler gibi çevresel ve harici etkiler sonucu oluşabilecek hasarlar ile kurum içi veya kurum dışından kaynaklanabilecek veri ve cihaz hırsızlığı (ya da kayıp) olaylarının kast edildiği bu siber tehdit türüne ilişkin olarak birçok kullanıcı diğer siber tehditlerle ilgili endişeler taşırken bu tehdidin oluşturacağı zararın farkında değildir.

B.9. APT (Advanced Persistent Threat)

Hedef odaklı geliştirilen, genellikle devletler veya hacktivist gruplar tarafından gerçekleştirilen geniş çaplı siber saldırılar olarak tanımlanan [21]. APT' lerin günümüzde istihbarat amaçlı olarak kullanıldıklarına ilişkin iddialar bulunmaktadır. Daha geniş bir ifadeyle; APT' ler, siber savunma sistemlerini kolaylıkla atlatabilen, hedeflere sızmak için gelişmiş teknikler kullanan, bulaştığı sistemlerde yayılarak uzun süre fark edilmeden çalışabilen, belirli sistemleri ve kişileri hedef alabilen, alanında uzman belirgin bir grup veya ülke tarafından geliştirilen yazılımlardır [1].

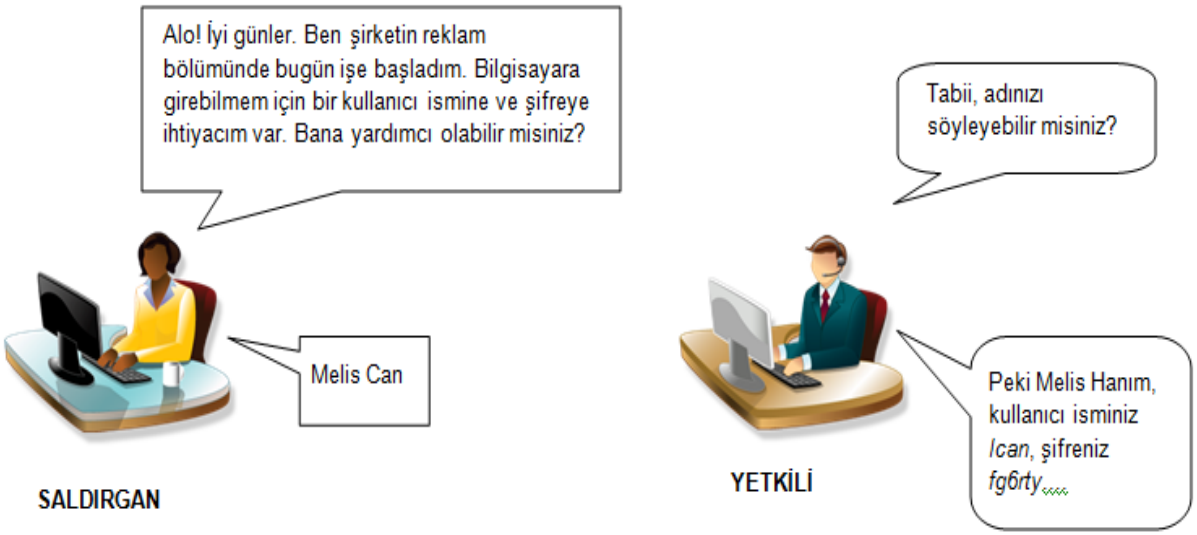
Genellikle hedef sistemlere sızarak bu sistemlerden veri aktarımı yapmak üzere programlanan APT' lerin en önemli özellikleri olarak enerji, ulaşım gibi belli sistemleri veya belli dillerde çalışan bilgisayarları hedef alarak bu sistemlere sızmaya çalışmaları ve birkaç virüs yazarı tarafından geliştirilemeyecek kadar karmaşık yapılara sahip oluşlarıdır [7]. Örneğin, İran nükleer sistemlerini kontrol eden bilgisayarlara sızan Stuxnet bu türden zararlı yazılımlara örnek olarak verilebilir.

B.10. Popüler Adresler Üzerinde Yapılan Saldırılar (Watering Hole)

2012 yılında RSA güvenlik firması tarafından tanımlanan bu tip saldırılar, saldırı yapılacak kurum veya şirket tarafından sıklıkla ziyaret edilen web siteleri tespit edilip, bunlardan biri veya daha fazlasına kötücül yazılımların (ya da zararlı kodların) yerleştirilmesiyle o kurum tarafından bu sitelere girilmesi neticesinde bu kötücül yazılımların (veya zararlı kodların) sistemlerine bulaştırılması yoluyla yapılmaktadır [18].

B.11. Sosyal Mühendislik

Sosyal mühendislik yönteminde, saldırgan hazırladığı sahte e-postalarla, telefonla ya da sohbet ortamları veya sosyal medyada kullanıcıyı kandırarak istediği bilgilere erişmeye çalışır. Ayrıca (özellikle ortak yazıcının kullanılması neticesinde) kurumda yapılan çalışmalarla ilgili alınan çıktıların değişiklik yapılmasından sonra gerekli şekilde imha edilmemesi sebebiyle kurum ve kurumun çalışmalarıyla ilgili büyük miktarda bilginin "çöplük karıştırma" diye tabir edilen yolla elde edilmesi ve kişilerin masalarında bıraktığı (kullanıcı adı, şifre ya da yapılan çalışmalarla ilgili v.b…) notlardan bilgi edinimi de sosyal mühendislik kapsamındadır [22]. Erkek sesine kıyasla kadın sesinin kullanılarak daha başarılı sonuçların elde edildiği sosyal mühendisliğe aşağıdaki gibi kısa bir örnek verilmesi uygun olacaktır [23]:



Şekil 3. *Sosyal mühendislik yöntemi*

B.12. Hizmet Aksattırma (DoS- Denial of Service)

Web uygulamalarının gereksiz yere meşgul edilerek normal işleyişinden alıkoyulmasına sebep olan hizmet aksattırma (Denial of Service) saldırıları ile kod enjeksiyonu kullanarak veritabanlarının işleyemez hale getirilmesi, web sunucusuna ait sistem kaynaklarının gereksiz meşgul edilmesiyle kullanıcıların erişememesi ve kimliklendirme ve yetkilendirme sistemlerinin kilitlenmesi sağlanabilmektedir. Örneğin, bir hastanede hastalara ait geçmişe yönelik muayene sonuçlarının tutulduğu veritabanı olsun. Bu veritabanından hastaya ait sosyal güvenlik numarasıyla yapılan sorgulama isteklerinin (onbinlerce kayıt taranması sonucunda) ekrana getirilmesi 1-2 dakika sürecek olursa (basit bir uygulama ile) böyle bir sorgulamadan eş zamanlı olarak 10 tane yapıldığında sistem kaynaklarını tüketeceğinden diğer kullanıcılar kayıtlara erişemeyecektir[15].

II. YÖNTEM

Bu çalışma ile siber tehditlerin etkilerinin artarak devam ettiği günümüzde kurumsal siber güvenlik kavramının net olarak anlaşılması, kurumsal siber güvenliğe yönelik tehditler hususunda farkındalık bilinci oluşturarak (veya arttırarak) bu tehditlere karşı etkin ve verimli mücadele yeteneği kazandırılması hedeflenmektedir.

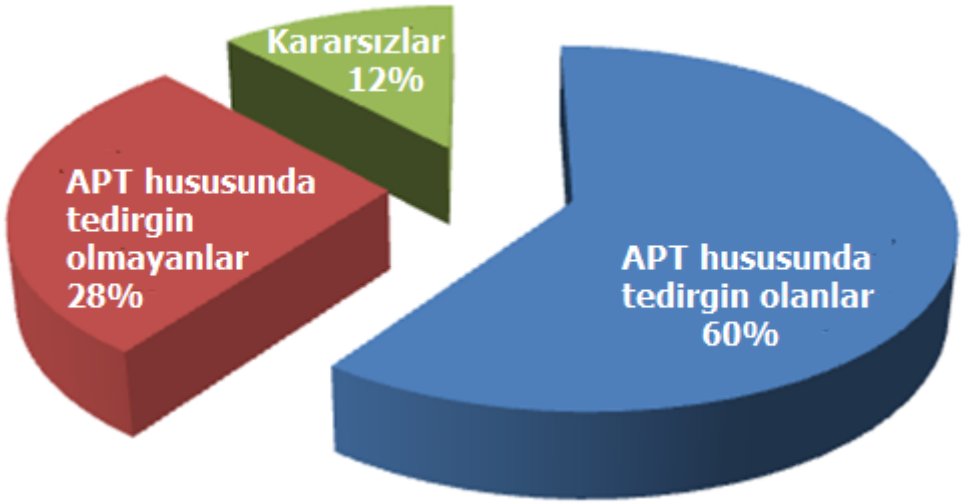
Ulaşılmak istenen verilerin elde edilmesinin zorluğu ve uzman görüşlerine olan ihtiyaç nedeniyle görüşme ve doküman analizi gibi veri toplama yöntemleri kullanılarak araştırmacının kendisinin veri toplamada kilit rolde olduğu nitel araştırma yöntemlerinden yararlanılmıştır. Bu bağlamda kurumsal siber güvenlik ve kurumsal siber güvenliğe yönelik tehditlere ilişkin (doküman analizi kapsamında) siber güvenlik alanında yetkinliğe sahip ulusal ve uluslar arası kurum ve kuruluşların sunduğu raporlar ile yerli ve yabancı çalışmalar incelenmiş, bu tehdit ve saldırılara karşı kurumsal bazda yapılabileceklere ilişkin olarakta yaşları 25 ile 35 arasında değişen ve 2-7 yıl arasında değişen görev sürelerine sahip siber güvenlikle ilgili birimlerde çalışan 10 personel ile görüşülmüştür.

III. BULGULAR ve TARTIŞMA

A. KURUMSAL SİBER GÜVENLİĞE YÖNELİK TEHDİT VE SALDIRILARA İLİŞKİN YAPILAN İNCELEMELER

Kurumsal siber güvenliği sağlamaya yönelik olarak (yukarıda bahsedilen) siber tehditlere ilişkin elde edilen bazı veriler aşağıda maddeler halinde sunulmuştur.

a-) Siber güvenliğe yönelik etkilerinin beklenin çok ötesinde boyutlarda olan APT' ler; birkaç virüs yazarı tarafından yapılamayacak şekilde gelişmişlik, karmaşıklık ve gizlilik gibi özelliklere sahip olmaları nedeniyle birçok kurum ve şirketin BT yöneticilerini, bilgi sistemlerini etkin bir şekilde koruyabilecekleri hususunda endişelendirmektedir(Şekil 4).

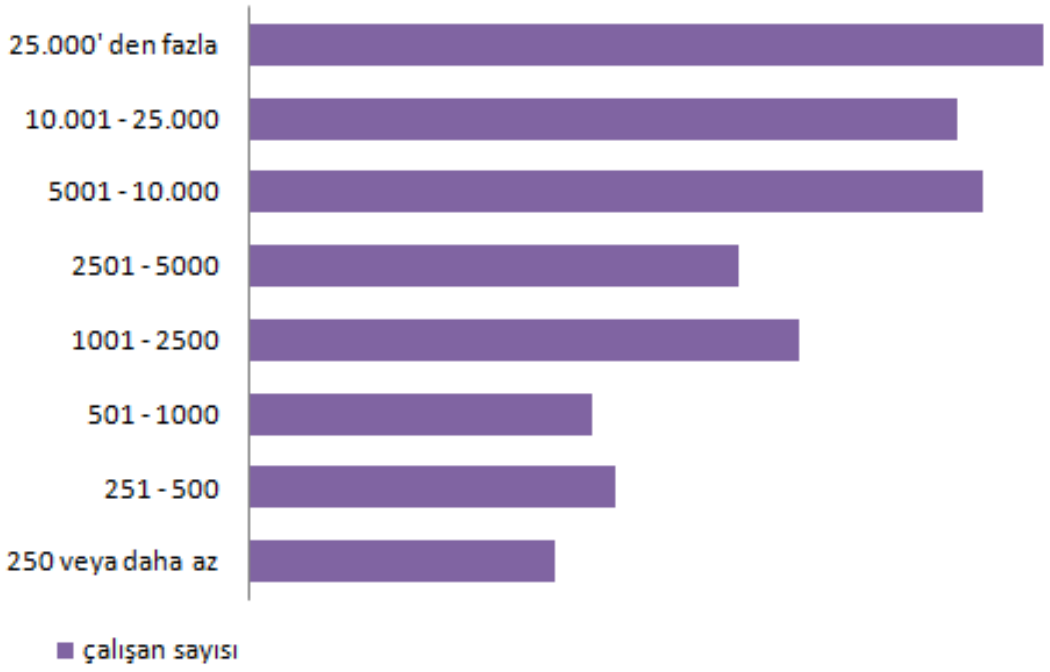


Şekil 4. *Kurum ve şirketlerin bilgi teknoloji uzmanlarının APT hakkındaki görüşleri*

b-) Yüksek teknolojiye sahip birçok şirket ile birlikte devlet kurumlarına başarılı saldırıların gerçekleştirilebildiği watering hole saldırı yöntemi, düşük sayıda gerçekleştirilse de yüksek başarı oranı ve bu tür saldırıların diğer saldırı yöntemleri ile birleştirilerek yapılması durumunda ortaya çıkacak etkili sonuçlar, tehdit analizi yapanları endişelendirmektedir [20].

c-) Kurumsal siber güvenlikte kurum ve şirketlerin karşılaştıkları en büyük tehditlerden bir haline gelen kötücül yazılımlara büyük ölçekli (25.000 ve daha fazla çalışanı olan) kurumların maruz kalma oranı küçük kurumlara oranlara (Şekil 5' de görüldüğü üzere) 2.5 kat daha fazla olmaktadır [3].

d-) Kurumsal siber güvenlikte en zayıf halkayı oluşturan insan faktörü üzerine odaklanan sosyal mühendislik yöntemi, çabuk sonuca götürmesi, hızlı ve basit olması nedeniyle saldırganlar tarafından sıkça kullanılmaktadır. Saldırganlar, bu yöntemi kullanmadan önce kurum hakkında bilgi toplamak için e-posta grupları ve forumları inceleyerek acemi ve sorumsuz sistem yöneticilerinin gönderdikleri mesajlardaki (gizli kalması gereken) bilgileri, bu ortamdaki gelişigüzel her sorunun açıkça sorularak yardım istenmesi sonucunda elde ettiği bilgileri ve arama motorlarını kullanarak yaptığı açık kaynak araştırması neticesinde edindiği bilgileri v.b. kullanarak hazırlık yapmaktadırlar.



Şekil 5. *Kurum ve şirket boyutuna göre kötücül yazılım risk durumu*

e-) Veri kayıplarının ana sebebinin hack olayları olmadığı, veri ihlallerinin % 36'sının cihazların kaybolması ve çalınması neticesinde gerçekleştiği sonucuna varılmıştır. Ayrıca mobil cihazlardaki kullanım artışının da etkisiyle (2013 yılında) hırsızlık ve kayıp olaylarında da artış olmuştur [20].

f-) Sazan avlama saldırıları coğrafi alanların kültürel, sosyal ve teknolojik gelişimlerine göre planlandıkları için bu tehditlerle mücadele de bu husus göz önüne alınmalıdır. Phishing (sazan avlama), web sitelerin güvenlik açıklıklarını kullandığında web uygulama güvenliğinin sağlanmasında uygulanan prosedürler önem kazanmaktadır.

g-) Ticari işlemlere erişim sağlamak için saldırganların kullanıcı bilgilerini kazanması ve oturumu ele geçirmesi şeklinde ifade edilen kimlik doğrulama ve oturum yönetimi ihlallerinin başarısı için ağ yapısı hakkında toplanabilecek bilgiler önemlidir. Ayrıca ağ yapısı hakkındaki bilgi farklı kaynaklar üzerinde depolanan verilere erişim için kolaylık sağlamaktadır.

h-) Veri ihlalleri ve bilgi sızıntısına ilişkin olarak; web sitesi geliştirilirken HTML kodları içerisinde silinmeden bırakılan tasarımcı notlarını bulabilmek için kodların satır satır incelenmesi ve web sitesindeki uygulamaların çalışma mantığını çözmek için yapılan çalışmalar saldırganların izlediği iki aşamalı bir yoldur [22].

i-) Bilgi ve iletişim sistemleri üzerinde yapılan dolandırıcılık faaliyetlerinde de kullanılabilen botnetler, zararlı yazılımların yayılmasında eskiye oranla daha az etkili olmasına rağmen en önemli siber tehditler arasında yer almaya devam etmektedir. Bunun nedeni kötücül yazılımların yayılma stratejilerindeki değişiklik olabileceği gibi, P2P teknolojisinin kullanımı da etkili olabilir. Web hosting servislerinin (çevrimiçi dosya depolama sağlayan bulut teknolojisi şeklinde) kullanımı botnetlerin etkinliğini arttırmaya neden olduğu ifade edilmektedir [20].

j-) Yapılan araştırmalara göre 7 binden fazla sahte anti virüs programının yer aldığı internette 30 milyondan fazla kullanıcı etkilenmiş durumdadır. Sahte antivirüs yazılımları arasında en bilinenleri PersonalAntiSpy, VirtualPCGuard, AntiMalware 2009 AntivirusProtection, Security Scanner 2008, VirusResponse Lab 2009, Antivirus Security, Micro Antivirus 2009 AntiSpyware Pro XP, XP Protector 2009, AV Security 2012, Windows Antivirüs 2011, AVG Antivirüs 2011, Protection Center, Vista Security Tool 2010, Antivirüs 8'dir [4].

A.1. Siber Tehditler ile Bu Tehditleri Gerçekleştiren Gruplar Arasındaki İlişkinin İncelenmesi

Siber tehditler ile bu tehditleri gerçekleştiren gruplar arasındaki ilişki Çizelge 1'de görülmektedir. Bu gruplar:

- Rekabet üstünlüğü elde etmek için siber tehditleri kullanarak rakiplerinin plan ve stratejilerini ele geçirme, gizlilik içeren kurumsal bilgilerine sahip olma gibi faaliyetler de bulunabilen ve hatta bunun için kendi siber yeteneklerini geliştirme çabası içinde olabilen *kurum ve şirketler*,
- Özellikle kendi siber yeteneklerini geliştirerek rakip devletlerin kamu ve özel şirketlerine karşı saldırılar yapan, kritik alt yapıları tehdit etme, devlet sırları ve askeri istihbarat bilgileri elde etme amacıyla (başarı oranı oldukça yüksek) saldırılar yapabilen *devletler*,
- Amaçları belirli uygulamaları protesto etmek veya (medyanın ve toplumun dikkatini çekecek şekilde) savundukları fikirlerini açıkça ortaya koymak olan ve medyanın dikkatini çekmekten hoşlanan, ideolojik olarak bir araya gelen grupların oluşturduğu *hacktivistler*,
- Bir ülkenin özellikle kritik alt yapılarına yönelik eylemde bulunmak amacıyla saldırı düzenleyen *siber teröristler,*
- Bir kurum ve şirketi yasadışı şekilde mali zarar uğratarak maddi kazanç sağlama eğiliminde olan, ayrıca yeteneklerini geliştirmek için bilgi paylaşımında bulunabilen ya da belli bir hedefe saldırı da bulunmak için kollektif hareket edebilen *siber suçlular*,
- Özellikle hacktivist grupların ve siber suçluların yaptıklarından etkilenerek ne kadar çok kod öğrenirsem o kadar hack eylemi yapabilirim düşüncesi içinde bulunan genç yaştaki saldırgan grupların oluşturduğu *script kiddle* (Bunlar buldukları hazır kodları ve uygulamaları kullanarak özellikle DoS atakları ve kod enjeksiyonu gibi saldırılarda bulunurlar.)
- Siber saldırılarda sosyal mühendisliğin artmasıyla önemli bir rol oynamaya başlayan, hedef personelle iletişim kurma, güvenini kazanma ve hedefle ilgili psikolojik ve sosyolojik analiz yapabilme yeteneğine sahip olan *çevrim içi sosyal hackerlar* (Bu grupların teknik bilgileri düşük olmasına karşın sosyal mühendislik yeteneklerinin yüksek olmasından dolayı (özellikle de sosyal ağların kullanımının artmasından dolayı) bu grupların saldırılarının artması beklenmektedir.)
- Elde ettikleri erişim hakları nedeniyle kurumsal bilgi varlıklarına yüksek oranda zarar verebilen fakat genellikle teknik düzeyi düşük (kötü niyetli ve kasıtlı) saldırılar yapan *kurum çalışanları* (kasıtsız olarak güvenlik ihlaline sebebiyet veren bilinçsiz kullanıcılar da bu kategoriye dahil edilmektedir.)
- Yüksek milliyetçilik ve kutsal devlet anlayışına sahip ve bu bilinçle bir takım saldırılarda bulunan *siber savaşçılar*dır.

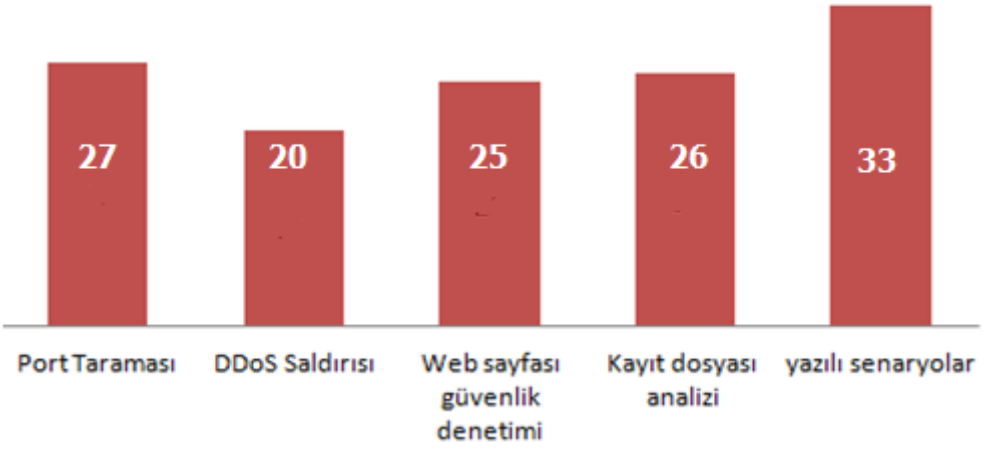
Siber tehditler arasında sahte antivirüs yazılımlarının yalnız siber suçlular ve izinsiz indirmelerin de siber suçlular ile devletler tarafından kullanılması dikkat çekerken bilgi sızıntısı, kimlik hırsızlığı ile hırsızlık ve kayıp gibi tehditlerin tüm gruplar tarafından kullanıldığı görülmektedir. Başka bir hususta; kurum veya şirketler tarafından sıklıkla ziyaret edilen web sitelerini hedefleyen ve yüksek teknolojiye sahip birçok kuruma başarılı saldırıların gerçekleştirilebildiği popüler adresler üzerinden yapılan saldırıların (watering hole) kısa zaman içinde birçok grup tarafından kullanıldığıdır.

Çizelge 1. *Siber saldırı ve tehditler ile bu tehdit ve saldırıları gerçekleştiren gruplar arasındaki ilişki[20]*

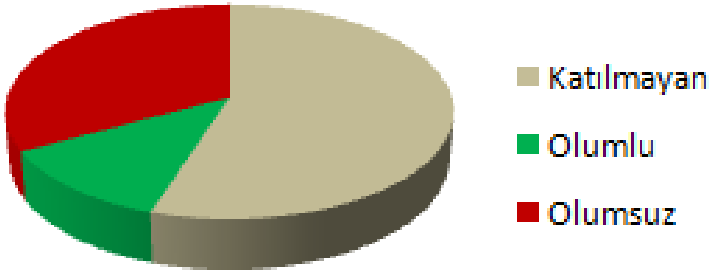
	TEHDİTLER	**Kurum ve Şirketler**	**Devletler**	**Hacktivistler**	**Siber Teröristler**	**Siber Suçlular**	**Siber Savaşcılar**	**Script kiddle**	**Çevrimiçi Sosyal Hackerlar**	**Kurum Çalışanları**
1	İzinsiz indirmeler		✓			✓				
2	Solucan/ Trojan		✓		✓	✓	✓		✓	✓
3	Kod enjeksiyonu	✓	✓	✓	✓	✓	✓	✓		
4	Exploit kits			✓	✓	✓	✓	✓		
5	Botnet	✓	✓	✓	✓	✓	✓			
6	Fiz.zarar ve hırsızlık, kayıp	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Kimlik hırsızlığı	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	Hizmet aksattırma		✓	✓	✓	✓	✓	✓		✓
9	Sazan avlama	✓	✓			✓			✓	
10	Spam	✓				✓			✓	
11	Sahte antivirüs yazılımı					✓				
12	Veri ihlali	✓	✓	✓	✓	✓	✓	✓		✓
13	Bilgi sızıntısı	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Hedefli saldırılar-APT)	✓	✓	✓	✓	✓	✓		✓	
15	Watering hole	✓	✓			✓	✓			

A.2. Kurumsal Siber Güvenliği Sağlama Adına Kurumsal Bazda Görülen Eksiklikler ve Yanlışlıkların İncelenmesi

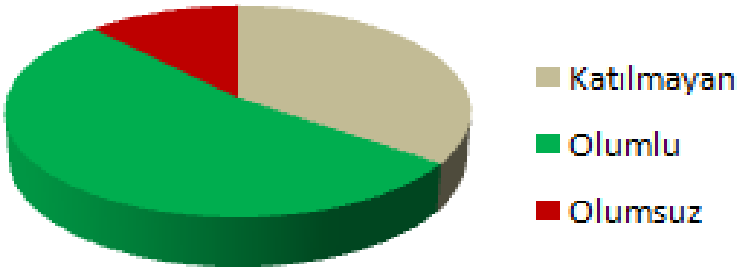
Ülkemizde siber tehditlere karşı hazırlıklı olunması, kurumların bilgi sistemi güvenliği olaylarına müdahale ve kurumlar arası koordinasyon yeteneklerinin tespit edilmesi, ulusal siber güvenlik bilincinin arttırılması ve kurumların bilgi ve iletişim sistemlerinin güçlendirilmesi amacıyla TÜBİTAK ve BTK işbirliğiyle (belirli aralıklarla) ulusal siber güvenlik tatbikatları düzenlenmektedir [13]. Bu tatbikatlardan çok sayıda kurumun katılım yaptığı, gerçek saldırı ve yazılı senaryoların uygulandığı 2011 yılındaki tatbikata ait bazı veriler aşağıdaki gibidir (Şekil 6-9).



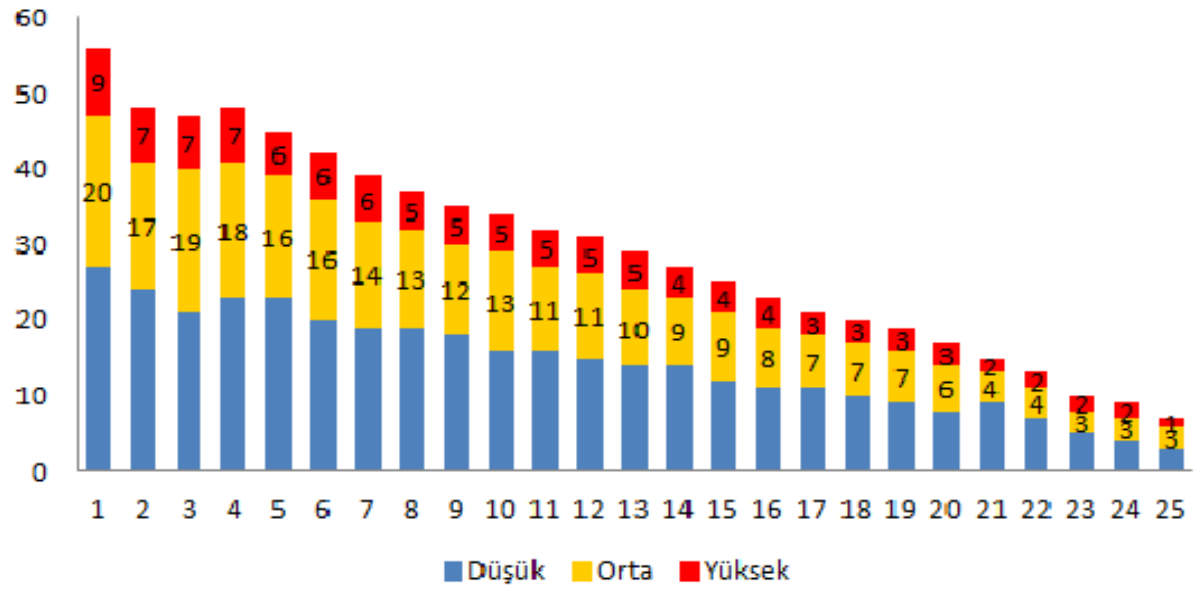
Şekil 6. *Gerçek saldırı ve yazılı senaryoların uygulandığı kurum sayısı*



Şekil 7. *DDoS saldırısının sonuçları*



Şekil 8. *Port tarama saldırısının sonuçları*



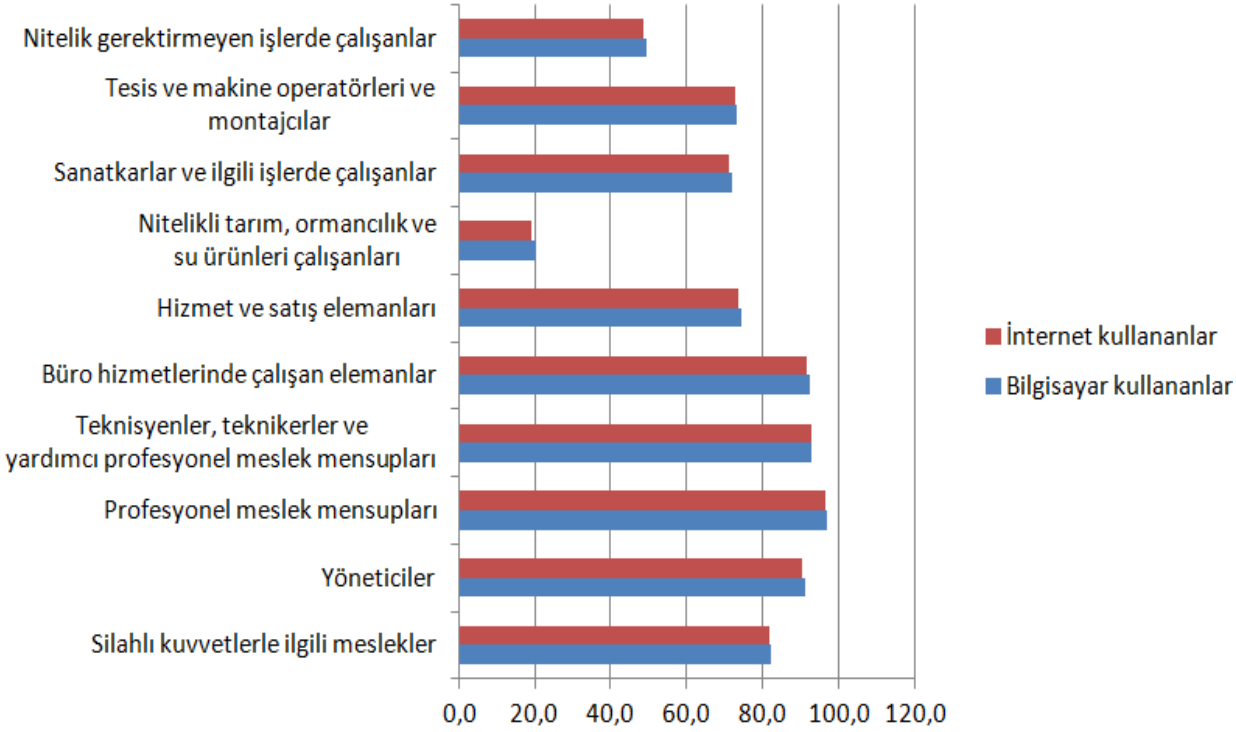
Şekil 9. *Kurumlarda tespit edilen web açıklıklarının sayıları*

Bu tatbikatlar sonucunda kurumlara ilişkin olarak [2]:

- Bazı kurumlarda bilgi güvenliği politikalarının olmadığı, saldırı esnasında ve sonrasında ne tür faaliyetler icra edileceğine dair siber güvenlik kültürü oluşturulmadığı
- Sistem yöneticilerinden birçoğunun yeterli teknik bilgiye sahip olmadığı
- Bazılarında STS (Saldırı Tespit Sistemleri) olmadığı olanlarda ise saldırıların tespitinde sıkıntılar yaşandığı
- Bazılarında teknik çözüm arayışına önem verilirken) sosyal mühendislik saldırılarına karşı personelde farkındalık eksikliği bulunduğu
- Antivirüs yazılımlarının düzenli olarak güncellenmediği
- Bazılarında iletişim hususunda eksiklikler bulunduğu, saldırı anında gerekli adımların atılması konusunda sıkıntılar yaşandığı ve ilgili mercilerle temas kurmada problemler olduğu
- Bazı personellerin kurumda (erişim izni olmadığı halde) kendisiyle ilgili olmayan hizmetlere erişebildiği
- Bazılarında sistem tasarım aşamasında güvenliğin temel bir tasarım ilkesi olarak ele alınmamasından dolayı güvenlik olayları yaşandığı ve bu olaylara etkin müdahalenin zorlaştığı
- Bazılarının (yaşanan sistem kesintisine yol açan güvenlik olayı neticesinde) iş süreçlerinin devamlılığını sağlayacak iş sürekliliği planına sahip olmadıkları
- DDoS (Distributed Denial of Service) saldırısı sonucunda bazı kurumların hizmetleri kesintiye uğrarken, İSS (İnternet Servis Sağlayıcı)' lerden bu tür saldırılara karşı hizmet satın alanların sıkıntı yaşamadığının görülmesi sonucunda kurumlar arası iletişime, işbirliğine ve koordinasyona verilmesi gereken önemin yeterince anlaşılamadığı
- Birçoğunun web uygulamalarında çeşitli açıklıklar bulunduğu, nispeten daha az güvenlik açığı bulunanların ise web uygulamalarını farklı kurumlara denetlettirdiği ya da web uygulamalarını geliştirirken güvenliğe dikkat ettikleri
- Özel bir bilgi güvenliği birimlerine sahip olan kurumların yapılan saldırıları analiz etmede daha başarılı oldukları
- Bazı kurumların da ulusal mevzuat hususunda yeterli bilgiye sahip olmamalarından dolayı yazılı senaryolarda siber suç olarak tanımlanan fiilleri adli mercilere bildirmedikleri tespit edilmiştir.

B. KURUMSAL SİBER GÜVENLİĞE YÖNELİK SİBER TEHDİTLERE KARŞI KURUMSAL BAZDA YAPILABİLECEKLER

Boyutuna bakılmaksızın tüm kurum ve şirketlerin siber güvenlikleri için önemli bir risk haline gelen siber tehditlerle ilgili her kurum ve şirketin (başta ağ yapısı ile ilgili olmak üzere) kurumsal güvenliklerine ilişkin gerekli, tedbirleri alması gerekmektedir. Ayrıca çeşitli meslek gruplarına göre bilgisayar ve internet kullanma oranlarının farklılaştığı ülkemizde (Şekil 10) siber suçluların; hedefledikleri kurumlardaki çalışanların internet alışkanlıklarını irdeleyerek elde ettikleri verilere göre çeşitli saldırılar gerçekleştirmeleri saldırının etkisini ve kurumsal siber güvenliğe verdiği zararı arttırmaktadır. Bilgisayar ve internet kullanma oranı nispeten daha yüksek olan kurum ve şirketlerdeki personelin farkındalığının arttırılması ve buralardaki siber güvenlikten sorumlu personellerin daha etkili çözüm önerileri geliştirip uygulamaları gerekmektedir. Ayrıca kötücül yazılım bulaştırarak kurumsal siber güvenliğe zarar vermek isteyen siber suçlular, sosyal ağların ve çevrimiçi video uygulamalarının personellerin işteki zaman geçirme alışkanlıklarını etkilemelerinden faydalanarak yeni güvenlik zafiyetlerinin oluşmasını sağlayabilmektedirler.



Şekil 10. *Meslek gruplarına göre bireylerin (16-74 yaş arası) bilgisayar ve İnternet kullanım oranları*

Siber ortamda sayıları her geçen gün daha da artan siber tehditleri bertaraf etmek, kurumsal olarak hizmet sunulan kitlenin memnuniyeti ve kaliteli hizmet anlayışı açısından önem arz etmektedir. Siber ortamda sunulan hizmet ve ürünlerin etkin, kaliteli ve uygun maliyetli olmasının yanında güvenliğin de tesisi önemlidir. Bu bağlamda yapılan görüşme de "Kurumsal siber güvenliği sağlama adına kurumsal bazda yapılabilecekler nelerdir?" sorusuna karşılık bir uzmanın vermiş olduğu:

"*…Bir kurum veya şirket için güvenlikten tasarruf edilemeyeceği gibi güvenlik endişesiyle sistem verimliliğini sağlayacak alt yapıların kullanımından da vazgeçilemez*." İfadesi ile yine bir başka uzmanın:

"*…Kurumların kendi içlerinde veya aralarında bir ar-ge çalışması yürütmemeleri ve bunun devletçe desteklenmemesi sonucu oluşacak dışa bağımlılık ulusal güvenlik adına tehditler oluşmasına yol açabilmektedir."*

şeklinde belirttiği görüş; güvenlik ile kullanılabilirlik arasındaki dengeyi ve kurumsal siber güvenliğin ulusal güvenliğe olan etkisini açıklayıcı niteliktedir. Yapılan görüşmelerde hemen hemen tüm uzmanlar;

- Personelin belirli çalışma alanlarına giriş izni yetkileri, oda ve binanın herhangi bir bilgi hırsızlığına maruz kalmayacak şekilde yalıtımı, kablolama güvenliği v.b. *fiziksel önlemler*
- Lisanslı ve güvenilir yazılımlar kullanılması, bilgisayarların sistem ayarlarında yapılacak düzenlemelerle harici bellek, CD-DVD ve disket gibi depolama birimlerinin kullanımının kontrol altına alınması gibi *işlemsel önlemler*
- Güvenlik duvarları, antivirüs programları, saldırı tespit ve önleme sistemleri, DoS (Denial of Service) engelleme sistemi v.b. *yazılımsal ve donanımsal önlemler*

şeklinde belirtilen korunma tedbirlerini[1] her kurumun (özellikle kritik bilgi ve iletişim sistemleri altyapısına ait bilişim sistemleri için) mutlaka yerine getirmesi gerektiğini ifade etmektedir. Ek olarak, (verilen cevaplar doğrultusunda) atılması gereken adımlar da şu şekilde belirlenmiştir:

1- Kurumsal siber güvenliğin sağlanması hususunda hem kurum departmanlarının görev, yetki ve sorumluluklarını belirleyen hem de ihtiyaç duyulan noktalarda eksiklikleri gidermek amacıyla yönetmelik oluşturulmalıdır. Yönetmelikte geçen kavramların net anlaşılması maksadıyla teknik terimler açıklamalı olarak verilmelidir.

2- Saldırılar neticesinde hukuki olarak netice alabilmek için siber saldırıların kaynağının tespit edilmesi hangi boyutta bir etki oluştuğunun bilinmesi gerekmektedir. Bu nedenle zamanın teknolojisine uygun olarak güvenilir ve yeterli kayıt mekanizmaları kullanılmalıdır.

3- Siber ortamda oluşan tehditlerin hızla belirlenmesi, yaşanabilecek saldırı etkilerini azaltmaya veya ortadan kaldırmaya yönelik tedbirlerin alınması için siber güvenlik birimi oluşturularak kurumun saldırı ve tehditlere müdahale yeteneği kazanması sağlanmalıdır. Ayrıca kurum veya şirketin ürün veya hizmet sunduğu sektörel çeşitliliğe bağlı olarak siber güvenlik birimine bağlı alt birimler kurulmalıdır.

4- Kritik bilgi ve iletişim sistem altyapıları başta olmak üzere departman bazında siber güvenliğin sağlanması adına çalışmalar yapılmalıdır.

5- Asıl mesele kritik bilgi ve iletişim sistem altyapılarına sızma ve keşif, veritabanlarını ele geçirme gibi saldırılar olduğundan, özellikle bu hususlarda kapsamlı bir risk değerlendirilmesi yapılması gerekmektedir.

6- Gerek ulusal gerekte uluslararası boyutta siber güvenlikle ilgili eylem planları, bildiriler ve konferanslar yakından takip edilerek edinilen bilgilerin kurumun siber güvenliğine uyarlanmasına çalışılmalıdır.

7- Özellikle kurumun kritik bilgi ve iletişim sistem altyapılarına ait bilişim sistemlerinin güvenliğini sağlamak maksadıyla oluşturulacak siber güvenlik eylem planının güncel gelişmeler doğrultusunda belirli periyotlarla güncellenmesi sağlanmalıdır.

8- Eylem planı ile ilgili olarak şirketin tüm departmanlarında (bilinmesi gereken kadar prensibince) gerekli bilgilendirmeler sağlanmalıdır.

9- Kurum olarak bilgi güvenliğine yönelik gerekli politikalar belirlenerek standartlar oluşturmalı ve bu konuda yönetmelik hazırlanarak personele tebliğ edilip farkındalık oluşturulmalıdır. Bu

[1] Kurumsal siber güvenliği sağlama adına (kılavuz niteliğinde) genel bir çerçeve oluşturmak amacıyla yapılan bu araştırmanın içeriğini gereğinden fazla detaylı kılacağı göz önünde bulundurularak bu korunma tedbirlerinden bahsedilmemiştir.

politikaları belirleme de kurum alt birimlerinde de kurullar oluşturularak onların destek ve önerilerinin alınması belirlenen politikaların benimsenmesinde etkili olacaktır. Ayrıca belirlenen bu politika ve yönetmeliklerin uygulanıp uygulanmadığı kurumun siber güvenlik birimince denetlenmelidir.

10- Ulusal ve uluslararası hukuk kuralları çerçevesinde kurumun haklarını korumak için herhangi bir saldırı durumunda saldırının kaynağının tespiti ve etki boyutunu ortaya koyacak saldırı tespit sistemleri ve güvenilir kayıt mekanizmaları oluşturularak günün teknolojisine uygun olarak güncellemeleri yapılmalıdır.

11- Kurumsal siber güvenlik birimine (KSGB) bağlı olarak görev yapmak üzere 7/24 esasına göre oluşturulacak kurumsal siber olaylara müdahale biriminin(KSOM), gerek diğer kurumların siber güvenlikten sorumlu birimleriyle gerekte ulusal boyutta siber güvenlik hususunda çalışma yapan birimlerle yakın işbirliği içinde olmaları sağlanmalıdır. Siber olaylara müdahale biriminde bulunan kişiler güncel gelişmeler doğrultusunda hizmet içi eğitim veya kurslarla en son gelişmelere adapte olacak şekilde yetişmeleri sağlanmalıdır.

12- Kurumun kritik bilgi ve iletişim sistem altyapılarındaki bilişim sistemlerinin, kritiklik seviyeleri, birbirleriyle ilişkileri ve sorumluları belirlenmelidir. Ayrıca bu kritik bilgi ve iletişim sistem altyapılarının güvenliği idari tedbirlerle de desteklenmelidir.

13- Kurumsal siber güvenliği sağlama konusunda departmanların farkındalık ve yetkinlik düzeyini arttırıcı teknolojik ve idari boyutta destek verilmelidir.

14- Siber güvenlik sadece teknik bir konu olarak ele alınmamalı, kurumu etkileyecek tüm sosyal ve ekonomik yönleriyle değerlendirilmelidir. Kurum içinde belirli zamanlarda "siber güvenlik farkındalık haftası" gibi etkinlikler doğrultusunda konuyla ilgili çalışmalar yürütülmelidir.

Ek olarak, kurumsal siber güvenliği sağlama adına artı değer katabilecek bazı adımları da şu şekilde sıralamak mümkündür [20]:

- Kurumlar işbirliği yaparak ortaya çıkan tehditlerle ilgili bilgi paylaşımında bulunmalı, yardımcı olmalı… Kurumlar arasında ortak bir bilgi toplama, analizi, değerlendirimi ve doğrulamasının yapılması gereklidir. Bu şekilde güvenlik kalitesi ve tehdit değerlendirme hızı artacaktır. Kamu ve özel sektörün bir arada bulunduğu çalışmaların yapılması bu tür tehditlere karşı daha etkili güvenlik mekanizmalarının oluşturulmasını sağlar.

- Tehdidin sebebiyet vereceği etkiyi azaltmak için tehdit değerlendirme hızı arttırılmalı. Ortaya çıkan tehditler hakkında sağlıklı bilgi elde etmek ve bu tehditlere yönelik güvenlik çözümleri geliştirmek maksadıyla yapılacak faaliyetlerle ilgili birimler kurulması ve geliştirilmesi önemlidir. Hayati öneme sahip tehdit değerlendirme hızının artışı için kurum ve şirketlerin oluşturacağı sinerji ve bu sinerjinin eylemlere yansıması gereklidir.

- Teknolojinin ilerlemesiyle beraber saldırılardaki karmaşıklığın artmasından dolayı güvenlik mekanizmalarının daha sağlam olması için geliştirilmesi, ek tedbirler alınması gerekirken bilginin gizliliği, erişilebilirliği ve bütünlüğüne ilişkin alınan önlemlerin de kurumsal işleyişin verimliliğini azaltmayacak şekilde esnek olması gerekmektedir.

- Güvenlik kontrol ve politikaları geliştirmek için yapılan araştırmalara yönelik yatırım yapılmalıdır.

Tüm bu sayılan maddelere ilaveten (fiziksel, işlemsel, yazılımsal ve donanımsal) gerekli korunma tedbirleri yerine getirilerek, bu önlemlerin etkinliğini ölçmek ve uygun güvenlik çözümleri geliştirmek amacıyla belli periyotlarla bağımsız ve tarafsız uzman kurumlara penetrasyon (sızma) testleri de yaptırılmalıdır. Ayrıca günümüzde (özellikle yapılan saldırı ve tehditlerin web uygulamalarına doğru

kayması nedeniyle) kurumların internet ortamından gelebilecek tehlikelere karşı (ilave) uygulayabilecekleri maddeleri de şu şekilde sıralamak mümkündür [19]:

1- Web uygulamalarına yönelik çalışmalarıyla bilinen OWASP' ın Güvenli Kodlama İlkeleri belgesi, Güvenli Web Uygulamaları Geliştirme Kılavuzu belgesi kurum içi eğitimlerde kullanılarak yazılım geliştiricilerin bu esaslara uyup uymadıkları denetlenmelidir.

2- İnternet üzerinden gerçekleştirilen etkinlikler (kurumsal ağ üzerinde) sürekli olarak izlenmelidir. Bunun için kullanılan en etkin yöntem, basit ağ yönetim protokolü (SNMP) araçlarının kullanılmasıdır.

3- Web sistemleri dönemsel olarak sınama araçları ile taranmalı ve sınamaya ilişkin rapor teknik sorumlulara ulaştırılmalıdır.

4- Kurumsal ağların, web güvenliği altyapıları için kılavuzları ve standartları bulunması gerekmektedir.

5- Saldırganların sistemde yapabilecekleri değişikliklerin takibi açısından (Tripwire ve benzeri programlarla) kritik sistem dosyalarında yaşanan değişimler izlenmelidir.

6- Sunucu günlükleri (log), sunucu makineleri üzerindeki web sunucu yazılımı ve web uygulama güvenlik duvarı gibi çeşitli sistemlerin günlük içeriklerini içeren sunucu günlükleri (log) tutulmalıdır.

IV. SONUÇ

Verinin gizliliği, bütünlüğü ve erişebilirliğinin hedeflendiği kurumsal siber güvenlikte kurumun kritik bilgi ve iletişim sistemlerine ait alt yapılarda iş sürekliliğinin sağlanması amaçlanmaktadır. Kurumların hizmet sunumlarını elektronik ortamda sunmalarının zorunluluk haline gelmesiyle kurumsal siber güvenliğe yönelik tehditlerde de artış olmuştur. İzinsiz indirmeler (drive by download) ve (özellikle solucan/truva atı gibi) kötücül yazılımlar ile etkileri günümüzde beklenenin ötesinde boyutlarda gerçekleşen APT ve yüksek teknolojiye sahip birçok kuruma başarılı saldırıların gerçekleştirilebildiği watering hole saldırıları kurumsal siber güvenlik açısından en önemli siber tehditler arasında yer almaktadır. Bu tehditlere karşı teknik çözümlerin yanında siber güvenliğin en zayıf halkası olarak nitelendirebileceğimiz insan faktörü üzerinde kurumların yeterince önlem almadığı görülmektedir. Bu durumun farkında olan siber suçluların, çalışanların internet alışkanlıklarını irdeleyerek elde ettikleri verilere göre çeşitli saldırılar gerçekleştirmeleri saldırının etkisini ve kurumsal siber güvenliğe verdiği zararı arttırmaktadır. Ayrıca günümüzde (teknik düzeyi yüksek) mevcut uygulama ve yazılımları kullanarak düşük düzeyde bilgi birikimi ile siber saldırıların gerçekleştirilebileceği görülmektedir ki; bu durumda saldırı sayısının artması ve buna bağlı olarak hem kurum ve şirketlere hem de bireylere verilebilecek zararların da artması normal karşılanmalıdır. Siber tehditlere ilişkin tüm bu gelişmelerin yanı sıra bu tehditleri gerçekleştiren gruplar arasından; hazır kodları ve uygulamaları kullanarak özellikle DoS atakları ve kod enjeksiyonu gibi saldırılarda bulunan *script kiddle* ve yüksek milliyetçilik ve kutsal devlet anlayışına sahip ve bu bilinçle bir takım saldırılarda bulunan *siber savaşçılar* gibi saldırılarını arttıran iki yeni sayılabilecek tehdit grubunun varlığı kurum ve şirketlere yapılabilecek saldırıların arttırmasını mümkün kılmaktadır.

Tarafsız ve bağımsız kurumlarca (belirli periyotlarla) yapılacak güvenlik ve sızma testleri neticesinde görülen eksiklik ve yanlışlıkların düzeltilmesi etkin ve kaliteli bir kurumsal siber güvenliğin oluşturulması açısından önemlidir. Tüm bunların yanı sıra kurumsal siber güvenliğe yönelik tehditlerin ağ sistemlerinden web uygulamalarına doğru kayması, daha organize ve karmaşık yapıya bürünerek artması daha etkin ve verimli bir siber güvenlik anlayışı ve çözümü geliştirmeyi zorunlu kılmaktadır. Bu bağlamda güvenlik ve kullanılabilirlik arasındaki denge gözetilerek kurumsal siber güvenliğin yaşayan bir süreç olarak ele alınması gerekmektedir.

V. KAYNAKLAR

[1] B. Bahtiyar, *Gelişmiş Siber Silahlar ve Tespit Yöntemleri*, **Siber Güvenlik Konferansı 2012**, Ankara-Türkiye, (2012).

[2] BTK, TÜBİTAK, "Ulusal siber güvenlik tatbikatı sonuç raporu", ***BTK ve TÜBİTAK***, (2011), 10-15.

[3] Cisco Systems, "Cisco 2013 yıllık güvenlik raporu", ***CISCO INC***, (2013), 34-35.

[4] S.S. Çakır, M. Kesler, *Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımları*, **XIV. Akademik Bilişim Konferansı**, Uşak-Türkiye, (2012) 551-558.

[5] M. Gülmüş, *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, İstanbul-Türkiye, (2010).

[6] M. Gülnaz, *Kamusal web güvenliği*, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul-Türkiye, (2010).

[7] H. Hekim, O. Başıbüyük *Uluslararası Güvenlik ve Terörizm Dergisi* **4 (2)** (2013) 135-144.

[8] Teknolojileri ve İletişim Kurumu, http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php (*Erişim Tarihi: 02.12.2013*).

[9] Anonim, http://www.chip.com.tr/haber/sahte-antivirusler-cogaliyor_19760.html (*Erişim Tarihi: 15.12.2013*).

[10] Dokuz Eylül Üniversitesi Bilgi Sistemi, http://web.deu.edu.tr/sss/spam.html (*Erişim Tarihi: 29.12.2013*).

[11] Microsoft Güvenlik Merkezi, http://www.microsoft.com/tr-tr/security/pc-security/antivirus-rogue.aspx (*Erişim Tarihi: 21.01.2014*).

[12] Anonim, http://www.telekom.com.tr/v2/faydali-bilgiler/182-bilgisayar-solucanlari-worms (*Erişim Tarihi :15.12.2013*).

[13] TÜBİTAK(BİLGEM), https://www.bilgiguvenligi.gov.tr/dokuman-yukle/6.-kamu-kurumlari-bilgi-teknolojileri-guv.-konf./unal-tatar-tatbikatlar/download.html (*Erişim Tarihi : 13.12.2013*).

[14] Anonim, http://tr.wikipedia.org/wiki/Bilgisayar_solucan%C4%B1 (*Erişim Tarihi : 29.12.2013*).

[15] WASC, http://projects.webappsec.org/w/page/13246921/Denial%20of%20Service (*Erişim Tarihi: 27.12.2013*).

[16] Anonim, http://en.wikipedia.org/wiki/Blackhole_exploit_kit (*Erişim Tarihi :29.12.2013*).

[17] Anonim, http://en.wikipedia.org/wiki/Computer_worm (*Erişim Tarihi :27.12.2013*).

[18] Anonim, http://en.wikipedia.org/wiki/Watering_Hole (*Erişim Tarihi :27.12.2013*).

[19] E. Karaarslan, T. Tuğlular, H. Şengonca, *Kurumsal web güvenliği yapısı*, **Akademik Bilişim 2008**, Çanakkale-Türkiye, (2008) 239-244.

[20] L. Marinos, (2013) **DOI:10.2788/14231**.

[21] O. Uçar, *Hedef Odaklı Siber Saldırılar*, **Siber Güvenlik Konferansı 2013**, İstanbul-Türkiye, (2013).

[22] Y. Vural, *Kurumsal Bilgi Güvenliği ve Sızma (penetrasyon) Testleri*, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara-Türkiye, (2007).

[23] D. Yılmaz, *Bilişim Korsanlığı ve Korunma Yöntemleri*, 2. Baskı, Hayat Yayıncılık, (2004).

[24] Microsoft, "Microsoft Security Intelligence Report", ***Microsoft Corp.***, (2013), 83-88.