İZMİR DAYANIŞMA
İZMİR SERBEST MUHASEBECİ MALİ MUSAVİRLER ODASI
CHAMBER OF CERTIFIED PUBLIC ACCOUNTANTS OF İZMİR

Volume / Cilt: 8, Issue / Sayı: 1, 2025,
E- ISSN: 2687-5233
ISSN: 3023-654
URL: https://www.journals.gen.tr/dayanısma
DOI: 10.69599/izd.2746

Geliş / Received : 02.03.2025
Kabul / Acccepted : 28.03.2025

HAKEMLİ YAZILAR / REFEREED PAPERS

# SİBER SALDIRILAR VE SİBER GÜVENLİK DENETİMİ GEREKSİNİMİ

## *CYBER ATTACKS AND THE NEED FOR CYBERSECURITY AUDITS*

**Özer Kestane**

Öğr. Gör. Dr., Dokuz Eylül Üniversitesi, İzmir Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Türkiye
e-mail: ozer.kestane@deu.edu.tr

**Öz**

Bilişim teknolojilerindeki hızlı gelişme ve ilerlemeler günümüzde işletme faaliyetlerini de değiştirmiş, işletmeler ar-ge, üretim, pazarlama ve finansman gibi tüm alanlarda internet ve internet tabanlı uygulamaları kullanmaya başlamışlardır. Bu uygulama ve araçlar sayesinde yeni ürün ve hizmet tasarımlarını kolayca geliştirmek, pazarlama faaliyetlerini çok daha etkinleştirmek, finansal analizleri rahatlıkla yapabilmek, her alandaki veriyi dijital ortamlarda depolamak, saklamak ve istenilen anda veriye ulaşmak mümkün hale gelmiştir. Fakat bu avantajlar aynı zamanda siber saldırılara maruz kaldığı için çok yüksek riskler de doğurmakta, işletmeleri maddi ve manevi zarara uğratabilmektedir. Bunun için işletmeler siber güvenlik alanlarına oldukça yüksek yatırım yapmakta ve gerekli önlemleri almaya çalışmaktadır. Bu araştırmanın da amacı siber saldırı ve siber denetimler konusunda bir farkındalık yaratmaktır.

Araştırma, bir literatür taraması olup siber saldırılar, siber güvenlik, atak tipleri, standartlar konusunda bilgiler vermektedir. Bu bilgiler ışığında işletmelerin uğrayabileceği siber saldırıların neler olduğu, bu konuda ne gibi önlemler alınması gerektiği, dünya ve ülkemizdeki siber güvenlik standartları konusunda bilinç yaratılmaya çalışılmaktadır.

**Anahtar kelimeler:** Siber Güvenlik, Zararlı Yazılım, Atak Tipleri, Siber Güvenlik Standartları, Siber Güvenlik Denetimi

**Citation/Atıf:** KESTANE, Ö. (2025). SİBER SALDIRILAR VE SİBER GÜVENLİK DENETİMİ GEREKSİNİMİ. *İZMİR SERBEST MUHASEBECİ MALİ MÜŞAVİRLER DAYANIŞMA DERGİSİ*. 8(1): 41-49, DOI: 10.69599/izd.2746

**Corresponding Author/ Sorumlu Yazar:**
Özer Kestane
E-mail: ozer.kestane@deu.edu.tr

**Abstract**

Rapid developments and advances in information technologies have also changed business activities today, and businesses have started to use the internet and internet-based applications in all areas such as R&D, production, marketing and finance. Thanks to these applications and tools, it has become possible to easily develop new product and service designs, make marketing activities much more effective, make financial analyses easily, store and save data in every field in digital environments and access data at any time. However, these advantages also pose very high risks as they are exposed to cyber attacks and can cause financial and moral damage to businesses. For this reason, businesses make quite high investments in cyber security areas and try to take the necessary precautions. The purpose of this research is to create awareness about cyber attacks and cyber audits. The research is a literature review and provides information about cyber attacks, cyber security, attack types and standards. In the light of this information, it is tried to create awareness about what cyber attacks businesses may be subject to, what precautions should be taken in this regard, and cyber security standards in the world and our country.

**Keywords:** Cyber Security, Malware, Attack Types, Cyber Security Standards, Cyber Security Audit

## 1. GİRİŞ

İnsanlık tarihini gözden geçirdiğimizde, insanın kendini koruma ve hayatta kalma ihtiyacı günümüze değin sürmüş ancak her geçen gün daha yeni boyutlar kazanmıştır. Avcı toplayıcı bir düzenden tarım toplumuna geçiş ile yerleşik hayata geçen insan, korumak zorunda olduğu varlıkların sahibi olmuştur. Modern yaşama evrildikçe de uymak zorunda olduğu kurallar ve kanunlara maruz kalmıştır. Bu süreç artık korunma ihtiyacının boyutlarının çok çeşitlendiği bir dönemin kapılarını aralamıştır. Çünkü önceki dönemlerde sahip olduğu arazisini bir köpekle ve tel bir çit ile koruması mümkünken, modern dönemde sadece somut varlıklarını değil, dijital dünyadaki her türlü ayak izini de korumaya ve bu ihtiyacı giderecek çok daha güçlü güvenlik tedbirlerini almaya mecbur kalmıştır. Çünkü kişisel, kurumsal ya da toplumsal olarak sınırları olmayan gözle görülemeyecek farklı bir tehdidin varlığı hemen hemen herkesin bildiği bir gerçektir ve bu durum siber güvenlik kavramını doğurmuştur.

Siber güvenlik, tüm bilişim sistemlerini içine alan genel bir kavram olarak ortaya çıkmıştır ve siber saldırı, siber savaş, siber ordu gibi bir çok kavramı içinde barındıran bilgi güvenliği kavramından çok daha geniş bir anlam içermektedir. Ayrıca internet güvenliği, yazılım güvenliği, donanım güvenliği gibi birçok konuyu da içermektedir (Altınkaynak, 2018).

Günümüzde dijital dünyada gerçekleşen her türlü faaliyet izlenebilmekte, kaydedilebilmekte, tehdit olarak kullanılabilmektedir. Siber suç, bir bilişim siteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber suçun diğer suçlardan farklı olarak değerlendirilmesinin sebebi bir bilişim sistemi olmadan işlenememesi ve ağ bağlı cihazların kullanılması nedeniyle de sınırlarının çok geniş olabilmesidir. Siber suç bir bilişim sistemine izinsiz ve hukuka aykırı bir şekilde girilmesi ve sonrasında gerçekleştirilen faaliyeti anlatır. Bu tür suçlarda hedef bir kişi olabileceği gibi, bir kurum, bir işletme, bir bölge, bir şehir, bir kıta ya da dünyanın büyük bir kesimi olabilir. Bir sisteme girerek verileri silmek, şifrelemek, ele geçirmek, zarar vermek, iletişimi izinsiz izlemek ve kayıt etmek gibi eylemler siber suçlar kapsamına girmektedir (Müdürlüğü, 2025).

İçeriden ya da dışarıdan girilerek bir şirketin resmi muhasebe kayıtları, fatura sistemleri ve diğer verilerinin başka bir ortama transfer edilmesi veya mevcut kayıtlarının silinmesi fiili de siber suç olarak adlandırılabilir.

Bilgi teknolojilerindeki baş döndürücü hız hayatın her yönünü etkilediği ve her meslekte, her alanda köklü değişimlere neden olduğu gibi bu değişimin yansımaları muhasebe mesleği ve bu meslekle ilgili her kurumu da etkilemiştir. Günümüzde gerek muhasebe kayıtları gerek-

se işletmeler için önemli yönetimsel ve finansal bilgiler dijital ortamlarda kaydedilmektedir. Bunun yanı sıra vergi mükellefi işletmeler için verilmesi gereken vergi beyannameleri başta olmak üzere, yevmiye defterleri ve kayıtları, faturalar, irsaliyeler, tahsilat makbuzları tüm belgeler elektronik ortamda oluşturulmakta ve elektronik olarak kaydedilmektedir. Elektronik ortama kaydedilen bu veri, teknolojiyi kullananlar açısından güvenlik boyutunda risklerin de oluşmasına neden olmaktadır. Bu nedenle siber suçlara karşılık siber güvenlik, şirketler, bireyler, kurumsal örgütler ve devletler için önemli bir konu haline gelmiştir (Özdemir, 2020). Verinin kaydedildiği ve işlendiği sistemlerdeki zayıflıkların, güvenlik zafiyetlerinin kötü niyetli kişi, kurum ya da topluluklar tarafından kullanılması, dünya çapında işletmelerin trilyonlarca dolar finansal kayba neden olduğu gibi güven kaybı, prestij kaybı, kurum itibarı gibi manevi anlamda da zarar görmesine neden olabilmektedir. Tüm kullanıcıların birbirleri ile hızlı etkileşim kurabildikleri bu dönemde gerçek olmayan bir haberin bile insanlar üzerinde oluşturduğu etki önemli sorunlara sebep olabilmektedir. Örneğin, dijital dünyada yaratılan asparagas bir haber nedeniyle haberle ilişkili sunucu üzerinde beklenenin çok üzerinde bir trafik oluşabilmekte, bu da ddos olarak adlandırılan siber saldırı türüne zemin hazırlayabilmektedir. Birçok kişi veya kurum bu suçun büyüklüğünden ve etkilerinden haberdar değildirler (Verma & Bajaj, 2008). Bu nedenle kişi ya da kurumların siber saldırılar konusunda bilinçlendirilmesi gerekmekte ve siber saldırıların önlenebilmesi ve bulunabilmesi amacıyla siber güvenlik denetimlerine ihtiyaç oluşmaktadır (Öztürk, Siber Saldırılar, Siber Güvenlik Denetimleri, 2018).

Siber güvenlik denetimi, bir kuruluşun güvenlik önlemlerini değerlendirip inceleyerek güvenlik açıklarını tespit etme, uyumluluğu sağlama ve hassas verileri koruma sürecidir (Dataguard, 2025).

Denetim süreci, kötü niyetli kişi, kurum ya da kuruluşların istismar edebileceği zayıflıkları ortaya çıkarmak için kullanılan iletişim kanallarının, bilişim sistemlerinin ve kullanılan uygulamaların detaylı incelemesini içerir ve bu sürecin devamlı olarak işletilmesini gerektirmektedir. **Çünkü** teknolojik değişimler ve yazılımlarda yapılan güncellemeler yeni zafiyetlerin oluşmasına neden olabilir, bu durum ise denetim sürecinin tekrarını gerektirir. Genel bir yaklaşımla sistemin yılda bir kez siber güvenlik denetiminden geçirilmesi öngörülmektedir. Ancak önemli derecede bir yazılım ya da sistemsel değişiklik durumu olduğunda iç ve dış denetim sayısı arttırılabilir. İç siber güvenlik denetimleri şirket içi güvenlik denetçileri tarafından gerçekleştirilir, hem maliyeti daha uygundur hem de dış denetimlerden daha hızlı ve daha verimlidir. Ancak, iç denetleme sürecini yürüten ekibin yetersizliği ya da iyimserliği bu süreçte olumsuzluklara neden olabilir. Aslında iç denetim, planlanan dış denetimin bir ön hazırlığıdır. Dış siber güvenlik denetimleri üçüncü taraf siber güvenlik şirketleri ve profesyonelleri tarafından yürütülmektedir. Dış denetçiler güvenlik protokolleri konusunda uzmanlıkları onaylanmış, belgelenmiş olmalıdır. Dış denetim, profesyonel bir süreç yönetimi sağlayacak, tarafsız sonuçlar elde edecektir, ancak sürecin maliyeti daha yüksek aynı zamanda koordinasyon sorunları yaşanabilecek bir ortam da oluşabilecektir. (Talents, 2025).

Siber güvenlik denetiminin amacı potansiyel siber tehditleri değerlendirmek için kapsamlı risk değerlendirmeleri ve güvenlik açığı taramaları yaparak güvenlik açıklarını tespit etmektir. Bu nedenle öncelikle bilinmesi gereken konuların başında siber saldırı araç ve yöntemleri gelmektedir.

## 2. SİBER SALDIRILAR

Kritik altyapı sektörlerine saldırma, hizmet dışı bırakma, oltalama, kötücül yazılımlarla zarar verme, sosyal mühendislik, ağ dinleme, veri sızdırma ve değiştirme gibi yöntemler ile devlet veya işletmelerin web hizmetlerini durdurma ya da aksatma, verileri değiştirme, silme, **çalma** veya paylaşma amacıyla hedef kişi, işletme veya kurumun iletişim ağlarına, iletişim cihazlarına veya bilgi sistemlerine siber ortamda yapılan genellikle planlı ve maksatlı saldırılara siber saldırı denir (Çakmak & Demir, 2009).

Siber tehditler, hedef aldığı organizasyonun, hükümet, işletme ve son kullanıcıların günlük

faaliyetlerini etkileyen tehditlerdir. **Örneğin, d**olandırıcılık faaliyetleri, müşteri veri ihlalleri, ATM'den usulsüz nakit çekimi gibi günlük faaliyetler veya etkileri uzun süre devam eden, ülkenin ve toplumun dengelerini değiştirmeyi hedefleyen, endüstriyel ve askeri casusluk, sosyal hoşnutsuzluk ve huzursuzluk yaratma, ulusal güvenlik ihlali gibi tehditlerdir (Yılmaz & Sağıroğlu, 2013).

## 3. ZARARLI YAZILIM

Zararlı yazılım kavramı, programlanabilir herhangi bir cihaza, hizmete veya ağa zarar vermek veya faydalanmak amacıyla tasarlanmış her türlü zararlı yazılım için kullanılan kapsamlı bir terimdir. Siber suçlular genellikle bunu, mali kazanç için kurbanlardan veri elde ederek baskı yapmak, çıkar sağlamak üzere kullanır. Bu veriler finansal verilerden sağlık kayıtlarına, e-postalara, kişisel bilgilere ve parolalara kadar değişebilir. Zararlı yazılım virüsleri de içeren her tür zararlı yazılımı kapsar ve kötüye kullanılabilecek bilgi türü sınırsızdır (Mcafee, 2025).

Teknolojinin gelişmesi ile her geçen gün yeni tür zararlı yazılımlar ile karşılaşmak mümkün olmaktadır. Günümüzde sıklıkla karşımıza çıkabilecek zararlı yazılım türlerinin başlıcaları ise virüsler, solucanlar (worms), casus yazılımlar (spyware), reklam yazılımları (adware), Truva atları (Trojen horses), botnetler, korsan amaçlı kullanılan yazılımlar (rootkits), fidye yazılımları (ransomware), arka kapılardır (backdoors) (Vodafone, 2025).

Genel anlamda zararlı yazılımlar 3 ana başlık altında analiz edilmektedir. Bunlar; statik analiz, dinamik analiz ve hybrid analizdir (Bbsteknoloji, 2025).

Statik analiz, zararlı yazılımın çalıştırılmadan yazılım ile ilgili bilgi toplanması işlemine verilen isimdir. Bu analiz yöntemi sayesinde bir dosyanın zararlı yazılım içerip içermediğini öğrenmek mümkündür. Dosya adları, IP adresleri, etki alanları gibi teknik göstergeler tanımlanır ve dosya başlığı verileri, bu dosyanın kötü amaçlı olup olmadığını belirlemek için kullanılabilir. Fakat bu analiz yönteminde zararlı yazılımın tam manasıyla amacı belirlenemeyebilir. Bunu belirleyebilmek için dinamik analiz yöntemi kullanılır (Sağıroğlu, Alkan, Samet, Ulutaş, & Yalman, 2018).

Dinamik analiz yöntemine, davranışsal analiz adı da verilir. Bu yöntemde zararlı yazılım çalıştırılır ve etkilediği yapı, meydana getirdiği işlemler, IP adresleri gibi bilgiler elde edilebilir. Bu analiz yöntemi kullanılırken tersine mühendislik tekniklerinden faydalanılır. Dinamik analiz, yazılım davranışını izleyerek sistemdeki hangi makine ve programların etkilendiğini, etkilenen programların eski haline nasıl döndürülebileceğini, sistemdeki hangi güvenlik zafiyetleri kullanılarak saldırının başladığını, hangi verilerin zarar gördüğünü, vb. sorularına yanıt vermek amacıyla yapılır. Bu yüzden zararlı yazılım çalıştırıldığında test edilen sistemlere ya da ağa zarar vermemesi için yalıtılmış konumda olması önemlidir (Bbsteknoloji, 2025).

Hibrit analiz, temel ve dinamik analiz tekniklerini birleştirerek, her iki yaklaşımın birlikte kullanılması ile daha avantajlı bir durum ortaya çıkmasını sağlamaktadır. Hibrit analizin davranışsal analiz tarafından oluşturulan verilere statik analiz uygulamaktır. Örneğin, kötü amaçlı bir kodun çalışıp bellekte bazı değişiklikler oluşturması gibi. Dinamik analiz ile bu durum algılanabilir ve böylece analistler geri dönüp bu bellek dökümü üzerinde temel statik analiz yaparak sorunun kaynağını belirleyebilir. Sonuç olarak, daha fazla güvenlik ihlali göstergesi elde edilebilecek ve sıfırıncı gün açıkları ortaya çıkabilecektir (Şirketi, 2021).

Zararlı yazılımlardan korunabilmek için alınması gerekli önlemlerin başında işletim sistemini ve uygulamaları güncel tutmak gerekmektedir. Sisteme sadece ihtiyaç duyulan ve düzenli olarak kullanılan uygulamalar yüklenmeli, kullanılmayan uygulamalar kaldırılmalıdır. Güvenlik sağlamak amacıyla geliştirilmiş güncel ve güvenirliği test edilmiş yazılımlar kullanılmaya dikkat edilmelidir. Ayrıca sistemin belirli aralıklarla yedeği alınmalı, güçlü parolalar kullanılmalı ve gizliliğin sağlanması gerekmektedir. Bununla beraber g**üvenilir ve gün**cel bir tarayıcı ve g**üvenli wi-f**i ağı kullanılmalıdır. Bilinmeyen kaynaklardan gelen e-posta ekleri açılmamalı, bilinmeyen bağlantılara tıklanmamalıdır (USOM, 2023).

## 4. ATAK TİPLERİ

Belirli bir amaca yönelik siber saldırılar olduğu gibi hedef gözetmeden de karşımıza çıkan virüsler vb. yapılar siber saldırıların farklı türlerinin göstergesidir. Siber tehditler üç ana başlık altında toplanabilir. Birincisi keşif atakları (reconnaissance attacks), ikincisi erişim atakları (access attacks) ve üçüncüsü servis dışı bırakma ataklarıdır (denial of servise -DoS- attacks) (Çallı, 2024).

İlk aşama olan keşif aşamasında, siber saldırganlar hedefleri hakkında bilgi toplamaktadırlar. Ağ yapısı, işletim sistemi, güvenlik duvarı, veritabanı sunucusu gibi bilgilere ulaşılırken bunların zafiyetlerinin tespit edilmesi, erişim elde etmek için gerekli olan kullanıcı bilgilerinin bulunmasına yönelik veriler elde edilmeye çalışılır. Özellikle hedef bir kurum, kuruluş veya KOBİ olması durumunda saldırganlar genellikle çalışanlara odaklanır ve hedefledikleri çalışanların sosyal medya hesapları üzerinde yer alan bilgilerini kopyalayarak hedefledikleri sisteme erişim elde etmeye çalışır (Çallı, 2024).

Bir sonraki aşama olan erişim atakları ise, önceki aşamada elde edilen bilgiler ile hedef sistemlere veya çalışanlara zararlı dosyalar, e-postalar veya kodlar iletilerek hedef sisteme erişim elde edilir. Elde edilen bu erişim ile bilgi sızdırma, ekleme, değiştirme, ifşa etme gibi temel düzeyde zararlar dışında birçok amaca hizmet edecek farklı durumlar da ortaya çıkabilecektir. Bu aşamada bir kişinin satın aldığı ürün, bu ürünü gönderdiği adres bilgisi bile kişisel mahremiyet açısından çok önemli bir veri olmaktadır. Bu toplum içindeki herhangi bir birey için bile önemli iken, konu tanınmış kişi ya da büyük bir kurum olduğunda çok daha farklı sonuçlar ortaya çıkabilecektir. Örneğin, herhangi bir kişinin kullandığı ilaç ya da tedavi süreci ile ilgili bilginin sızdırılmasından, ülkenin yönetimindeki bir kişinin sağlık bilgilerinin sızdırılması toplumu farklı şekillerde etkileyecek ve belki de o toplumun geleceğini değiştirecektir.

Servis dışı bırakma atakları ise sistemi ya da kurumu işleyemez hale getirmek amacıyla gerçekleştirmektedir. Amaç, sistem ya da kurumun dış dünya ile bağlantılarını koparmak ya da iş/işlem yapamaz hale getirmektir. Burada öncelikli olarak sistemin çalışmamasından kaynaklı bir zarar oluşmaktadır. Bir e-ticaret sitesinin çalışmaması o süre içerisinde işlemlerin yapılamaması anlamına gelmektedir. Bu süre içerisinden muhtemel yapılacak satış ve elde edilecek kazanç hesaplanıp, zarar olarak düşünülebilir, ancak müşteri güveninin kaybedilmesi, prestij kaybı gibi nedenlerden ötürü zarar bunun çok daha ötesinde olabilecektir. Eğer çalışması engellenen bir finans sistemi ise bu durumda kullanıcıların anlık olarak gerçekleştirmesi gereken ödeme, para transferi gibi işlemlerin yapılamamasının mali boyutları çok daha büyük zararlar oluşturabilecektir. Sağlık sektöründe bir sistemin çalışması engellendiğinde bir hastanenin tüm işlemlerinin aksamasına hatta ameliyatların yapılamamasına neden olabilecektir. Günümüzde hemen hemen her sektörde kullanılan tüm cihazlar yazılım ve internet desteği almaktadırlar. E-ticaret gibi tamamen sanal ortamda müşterilerine hizmet veren ve gelir elde eden işletmeler için hizmet durdurma (DoS- DDOS) saldırıları çok tehlikeli olmakla beraber beklenilenden de fazla maddi zararlar verebilecek kadar önemli sonuçlar oluşturmaktadır. Araştırma, geliştirme ve üretim yapan işletmelerin ticari sırlarını ve bilgi birikimini elde etmeye yönelik hedef odaklı saldırılar sonucunda hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi söz konusu olabilmektedir. 2010 yılında İran'da nükleer santralde gerçekleşen Stuxnet olayı olarak literatürde yer alan saldırı siber saldırıların boyutlarının uluslararası düzeyde olabileceğini ve tüm toplumu etkileyebileceğini gösteren ilk örneklerden birisi olmuştur (Şener, 2014). Mart 2021 tarihinde kayıtlara geçen bir diğer siber olay da yemeksepeti adlı sitenin verilerinin ele geçirildiğine dair haberlerdir. Bu olayda saldırganlar yaklaşık 22milyon kişiye ait bilgiyi ele geçirmişlerdir. Bu tür bir olay gerçek olmasa bile yapılan haberlerden endişe duyan kullanıcıların güven kaybına ve ilgili işletmenin prestij kaybına neden olabilmektedir (Çalışkan, 2021).

2023 yılında yapılan bir araştırmaya göre dünya genelinde 35 saniyede bir, yani günde 2244 siber saldırı gerçekleşmektedir. Dünyada siber saldırılardan en çok etkilenen ülkeler arasında Türkiye

5.sırada yer almaktadır (Yılmaz M. , 2023). Bir başka araştırmaya göre Türkiye'de 2023 yılının 3. çeyreğinde tespit edilen oltalama saldırıları 2023 yılının 2. çeyreğine kıyasla %20, 2022 yılının 3. çeyreğine kıyasla ise %47 oranında artmıştır. 2022 yılında Türkiye'deki IoT cihazlarına yönelik 27 milyondan fazla saldırı tespit edilmiştir. Bunlar arasında özellikle elektrik ve su sistemleri gibi akıllı şehir altyapı bileşenleri yer almaktadır (Kaspersky, 2023). Bu veriler nedeniyle tüm dünyada ve ülkemizde siber saldırıların zararlarını önlemek ya da en az etki ile bertaraf edebilmek için belirli standartlar oluşturulmuştur.

## 5. SIZMA TESTLERİ

Sızma testi, bilişim sistemlerini oluşturan ağ yapılarına, donanım, yazılım, veri tabanı ve uygulamalara kötü niyetli kişilerin saldırmasını öngören yöntemleri kullanarak yapılan saldırı ve müdahaleler ile güvenlik açıklarının belirlenip, bu açıklarla sisteme sızılmaya çalışılmasının simüle edilmesi ve tüm bu işlemlerin raporlanmasıdır (Aslanbakan, 2017). Yapılış türlerine göre sızma testlerinin de çeşitleri vardır.

Sızma testinin yapılacağı sistem için testi gerçekleştirecek olan sertifika ve izinlere sahip sızma testi uzmanı/kurumu ile gerçekleştirilecek testler, yapılacak incelemenin türüne bağlı olarak siyah kutu sızma testi, beyaz kutu sızma testi ve gri kutu sızma testi olarak üç farklı inceleme türüne sahip olmaktadır (Yalçınkaya & Küçüksille, 2017).

Siyah kutu sızma testinde, test edilecek sisteme, saldırganlar tarafından gerçekleştirilebilecek ve tamamen dışarıdan gelebilecek saldırıların birebir kopyasına karşılık dayanıklılık testleri gerçekleştirilmektedir. Test edilecek sistem hakkında hiçbir bilgiye sahip olmayan konunun uzmanları gerçek bir saldırgan gibi sistemin olası tüm dış saldırılara karşı güvenliğini test etmektedirler. Bu test türünde gerçek sistem üzerinde test yapıldığı için sistem zarar görebilir. Bu nedenle, testler öncesi sistemin güvenli yedeği alınmalı ya da sistemin birebir kopyası üzerinde testler gerçekleştirmelidir.

Beyaz kutu test türünde test uzmanına, sistem hakkında detaylı bilgi verilmektedir. Sistemin ip adresleri, ağ haritası, sunucu yazılımları ve aktif servisleri hakkında bilgiler, sistemde tanımlı kullanıcı ad ve şifreler gibi bilgiler kullanılarak testler gerçekleştirilmektedir. Bu test türünde sistem hakkında bilgiye sahip olabilecek olası saldırganların oluşturabileceği tehditleri bertaraf edebilmek için araştırmalar yapılmaktadır.

Gri kutu test türünde iç ağda bulunan yetkisiz bir kullanıcının sisteme neden olabileceği zarar ve hasarın analiz edilmesi sağlanır. Sistemden izinsiz veri elde edilmesi, var olan bir yetkinin seviyesinin yükseltilmesi, ağ trafiğinin izlenmesi ve kaydedilerek bilgi sızdırılması gibi konular testlere tabi tutulmaktadır. Bu test türü siyah kutu sızma testi ile beyaz kutu sızma testi arasında yer almaktadır. Testi gerçekleştirecek kişiler belirli bir seviyede sisteme ait bilgiye sahip olmak durumundalar.

## 6. SİBER GÜVENLİK STANDARTLARI

İşletmeler faaliyetlerini gerçekleştirirken birçok amaç ile bilgi teknolojilerini kullanmaktadırlar. Kullanılan teknolojiler genel olarak birbirine çok benzerlik gösterse de ülkeden ülkeye, sektörden sektöre, hatta işletmeden işletmeye değişiklik gösterebilmektedir. Dolayısıyla her bir işletmenin bilişim teknolojisi ve risk faktörü birbirinden farklılık göstermektedir. Bu nedenle denetleme faaliyetlerini yürütürken tutarlı bir çerçeveye ihtiyaç duyulmaktadır (Weiss & Solomon, 2015). Siber güvenlik standartlarının amacı işletmelerin riskleri ve güvenlik zafiyetlerini azaltarak, güvenilirliği artırmaktır. Bu amaçla hazırlanmış uluslararası düzeyde kabul görmüş çok sayıda standart ve düzenleme mevcuttur. ISO/IEC 27000 Serisi, COBIT, ITIL ve NIST Siber Güvenlik Çerçevesi gibi standartlar ve düzenlemeler, bu standart ve düzenlemelerden bazılarıdır (Güngör, 2021).

ISO/IEC 27001:2022, uluslararası bir standart olup organizasyonların bilgi güvenliğini en iyi **şekilde yönetmeler**ini sağlamak için gereklilikleri içermektedir. Bilgi güvenliği, siber güvenlik ve gizliliğin korunması, organizasyonların bilgi varlıklarını, bilgi süreçlerini, bilgi güvenliğini ve risk yönetimini korumak amacıyla bir dizi politika, süreç ve kontrolleri içeren bir yönetim yaklaşımını içermektedir. Bu standart, işletmelerin

bilgi güvenliği yönetim sistemini kurma, uygulama, sürdürme ve sürekli iyileştirme süreçlerini yönlendiren bir yapı oluşturmasını sağlar. Standartta, işletmelerin bilgi güvenliği politikalarını belirlemeleri, risk yönetimi süreçlerini uygulamaları, uygun güvenlik kontrollerini seçmeleri ve uygulamaları, bilgi güvenliği farkındalığını artırmaları ve sürekli iyileştirme faaliyetlerini gerçekleştirmeleri konusunda aksiyonlar alınması sağlanır (Yılmaz B. , 2025).

COBIT (Control Objectivesfor Information and Related Technology), 1996'da Information SystemsAuditand Control Foundation (ISACF) tarafından yayımlanmıştır. İş hedeflerinin, bilgi ve ilgili teknolojilerle uyumunu (Business-IT Aligment), sonuçlarını, etkinliğini, bütünlüğünü, verimliliğini, güvenilirliğini, gizliliğini vb. konularını izleyen, ölçen, denetleyen ve iyileştiren bir bilişim teknolojileri yönetişimi (IT Governance) metodolojisidir. Yöneticiler için destekleyici bir araç olacak şekilde tasarlanmış ve teknik konular, iş riskleri ve kontrol gereksinimleri arasındaki uyumu sağlamayı hedeflemektedir. Bu standart işletmelerdeki bilgi sistemlerinin kalitesini, kontrolünü ve güvenilirliğini sağlar (Tanın, 2025).

ITIL (Information Technologies Infrastructure Library), Bilgi Teknolojisi Altyapı Kütüphanesi anlamına gelmektedir. ITIL; HSBC, IBM ve hatta NASA dahil olmak üzere dünyanın en büyük şirketlerinden bazıları tarafından kullanılan bir dizi Bilgi Teknolojileri Hizmet Yönetimi (IT Service Management) uygulamasıdır. ITIL, BT yönetimi prosedürlerini standart hale getirmek ve işletmelerin mümkün olan en kaliteli hizmetleri sunmak amacıyla en bilinen tuzaklardan kaçınmalarına yardımcı olmak için tasarlanmıştır. Çeşitli düzeylere ve modüllere ayrılan ITIL, hizmet stratejilerinden sürekli iyileştirmeye kadar her süreci kapsar ve uygulayıcıların yalnızca bilişim teknolojileri altyapılarını uyarlamalarını sağlamakla kalmaz, aynı zamanda daha sonraki değişiklikler için çevikliklerini artırır. ITIL'in faydaları, hizmet geliştirme ve dağıtım masraflarının azaltılması, stabil hizmet sunumuyla müşteri memnuniyetinin artırılması, bilişim personelinin veriminin artması, kalite iyileştirmeleri, daha iyi hizmet yönetim metrikleri ve hizmetleri değişen iş gereksinimlerine uyarlamada artan esnekliği içermektedir (MOSAcademy, 2024) (Academy, 2025).

NIST Siber Güvenlik Çerçevesi, ABD Ticaret Bakanlığına bağlı Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından oluşturulan Cyber-Security Framework (CSF), uygulandığı kritik altyapıya sahip her türlü kuruluş/organizasyona uyum sağlayabilen, uygulandığında siber saldırıları önleme, tespit etme ve bunlara yanıt verme becerilerinin nasıl değerlendirileceği ve geliştirilebileceğine yönelik politika seviyesinde düzenleme sağlar. Bu düzenleme kuruluşlar için mevcut siber güvenlik duruşunu tanımlar, siber güvenlik için hedef durumların tanımlanmasını sağlar, sürekli ve tekrarlanabilir bir süreç bağlamında iyileştirme fırsatlarını belirler ve önceliklendirir, hedef duruma doğru ilerlemeyi ölçümler ve değerlendirir, iç ve dış paydaşlar arasında siber güvenlik riskleri hakkında iletişim kurulmasını sağlar (Cyberarts, 2025).

Günümüz bilgi çağında, her şeyin her an değiştiği ve yepyeni teknolojilerin hayatımıza her gün giriş yaptığı bu dönemde işletmelerin siber risklere tam anlamıyla hazır olamayacağı bu tür risklerden kaçınmanın neredeyse imkânsız olduğu bir gerçektir. Bu riskleri yönetebilmek adına ya da siber saldırıların öncüllerini belirleyebilmek adına etkin bir eylem planına ihtiyaç duyulmaktadır. İşletmelerde siber risklere uygun kontrollerin planlanması, tasarlanması ve uygulanması sonucunda oluşabilecek riskler ve etkiler minimize edilebilecektir (Kurt & Uysal, 2015).

Öztürk (2018) yaptığı çalışmada, siber güvenlik ile ilgili bütüncül bir siber güvenlik denetim modeli önerisi geliştirmiştir. Modele göre siber güvenlik denetimlerindeki en önemli sorumlular, işletmelerin yönetim birimleri, risk yönetim birimleri ve iç denetim komiteleridir. Bu süreçte işletme yönetimi, en üst düzey yönetici konumunda bulunmaktadır. Risk yönetim birimi, işletmenin karşılaşabileceği siber tehditlerin ve denetim risklerinin ortaya çıkarılıp yönetilmesinde rol almaktadır. İç denetim birimi siber tehditlere karşı iç denetim mekanizmasının hazırlanmasında, güvenlik önlemlerinin yürütülmesinde, siber güvenlik denetim faaliyetlerinin yerine getiril-

mesinde ve üst yönetimle iletişim kurulmasında aktif rol almaktadır. Yönetimin desteği ve konu ile ilgili yönlendiriciliği olmadan siber güvenlik denetim faaliyetlerinin hedeflenen başarıya ulaşması olası değildir. Siber güvenlik denetimleri ile ortaya çıkan denetim raporu ile denetlenecek veriler, belgeler, dosyalar ve yazılımların işletme tarafından belirlenmiş olan standartlar, kurallar, ilkeler ve yürütülmekte olan güncel mevzuata uygunluğunun araştırılması sonucunda ortaya çıkmaktadır. Uygunluk konusunda sistemsel düzensizlikler ve açıkların bulunması durumunda güvenlik zafiyetinin varlığı ispatlanmış olmaktadır. Bu durum işletmeleri farklı açılardan zararlara uğratabilecek bir yapının varlığını işaret etmektedir. Yapılan siber güvenlik denetimi, belirlenen bir güven aralığında güvence verilebilmektedir. Denetim güvencesinin iyi olması, işletmenin siber güvenlik politikalarının da başarılı olduğunu belirtmiş olur (Öztürk M. S., 2018).

## 7. SONUÇ

Bilişim teknolojilerinin gelişmesi ile birlikte devletler günümüzde, tüm kamu kurumlarının hizmetlerini dijitalleştirerek bilgisayar ve internet ortamına taşımıştır. Kurumların tüm verilerini bilgisayar ortamına taşıması, güvenlik risklerini de beraberinde getirmektedir. İnternet üzerinden kullanıma açılan tüm bu veriler kamu düzeni ve güvenliği, kamu hizmetlerinin sürdürebilirliği açısından kritik altyapıların korunması gerekliliği doğurmaktadır. Günümüz şartlarında her bir birey de dijital dünyanın bir parçası olarak yaşamını sürdürmekte, dijital varlıklarının güvenliğini sağlamak durumunda kalmaktadır. Bununla birlikte iş dünyası ve ticari faaliyetlerin de bilişim teknolojileri ve dijital dünyanın avantajlarını kullanırken dijital varlıklarını korumak için siber saldırılara yönelik önlemler almak zorundadırlar. Çünkü, internet ağı sayesinde, özellikle bulut ortamında kaydedilen ve saklanan veriler zaman ve mekan sınırlaması olmadan kullanımı kolaylaştırmaktadır. Ancak bunlar aynı zamanda dışarıdan gelen saldırılara karşı da çok açıktır. İşletme sistemlerine dışarıdan gelebilecek bu saldırılar gerek maddi gerekse de manevi birçok problemi beraberinde getirebilmektedir. Siber güvenlik probleminin risklerini olabildiğince ortadan kaldırmak için öncelikli konulardan birisi siber güvenlik denetimidir. Siber güvenlik denetimi, saldırıların gerçekleşmeden önce nasıl önlenebileceğini araştırmayı, buna göre tedbir almayı gerektirmektedir. İşletmeler siber tehditler için mekanizmalar geliştirseler bile hızla gelişen bilgi teknolojilerine ayak uydurmak için aynı hızda aksiyon almayı gerektirmektedir. Bu sebeple siber güvenlik denetimi, siber saldırıları önlemek ya da oluşabilecek zararları olabildiğince azaltmak için gerekli hamlelerin atılmasını sağlayacak bir yapının temel taşlarıdır.

## KAYNAKÇA


Altınkaynak, M. (2018). *Uygulamalı Siber Güvenlik ve Hacking.* İstanbul: Abaküs.

Aslanbakan, E. (2017). *Bilgi Güvenliği ve Uygulamalı Hacking Yöntemleri.* 2. dü. İstanbul: Pusula.

Bbsteknoloji, (2025). *Bbsteknoloji.* [Çevrimiçi] Available at: https://bbsteknoloji.com/zararli-yazilim-analizi/ [Erişildi: 10 2 2025].

Çakmak, H. & Demir, C. K. (2009). Siber Dünyadaki Tehdit ve Kavramlar. %1 içindeH. Çakmak & T. Altunok, düz. *Suç Terör ve Savaş Üçgeninde Siber Dünya.* Ankara: Barış Platin Kitabevi, pp. 23-54.

Çallı, Y. (2024). *Siber Saldırı Nedir? Siber Saldırılardan Nasıl Korunuruz?.* [Çevrimiçi] Available at: https://berqnet.com/blog/siber-saldiri [Erişildi: 14 2 2025].

Dataguard, (2025). *Dataguard.* [Çevrimiçi] Available at: https://www.dataguard.com/cyber-security/audit/[Erişildi: 4 2 2025].

Mcafee, (2025). *Mcafee.* [Çevrimiçi] Available at: https://www.mcafee.com/tr-tr/antivirus/malware.html [Erişildi: 10 2 2025].

Müdürlüğü, E. G., 2025. *Siber Suç Nedir?.* [Çevrimiçi] Available at: https://www.egm.gov.tr/siber/sibersuc-nedir

Özdemir, M., (2020). *Muhasebe Finans Perspektifinde E-Dönüşüm Süreci.* 1 dü. Ankara: Nobel Yayın.

Öztürk, M. S. (2018). Siber Saldırılar, Siber Güvenlik Denetimleri. *Muhasebe ve Vergi Uygulamaları Dergisi*, Issue özel sayı, pp. 208-232.

Sağıroğlu, Ş. ve diğerleri. (2018). *Siber Güvenlik ve Savunma.* 1. dü. Ankara: Grafiker Yayınları.

Şirketi, O. B. G. v. Y. L. (2021). *Kötü Amaçlı Yazılım Analizi Nedir?*. [Çevrimiçi] Available at: https://www.ozztech.net/siber-guvenlik/kotu-amacli-yazilim-analizi-nedir/#:~:text=Hibrit%20analiz%2C%20temel%20ve%20dinamik,ihlali%20g%C3%B6stergesi%20(IOC)%20%C3%A7%C4%B1karabilir. [Erişildi: 10 2 2025].

Talents, C. (2025). *Siber Güvenlik Denetimi: Bilmeniz Gereken Her Şey*. [Çevrimiçi] Available at: https://cybertalents.com/blog/cyber-security-audit [Erişildi: 9 2 2025].

USOM, U. S. O. M. M. -. (2023). *Bireysel Siber Güvenlik Yöntemleri.* [Çevrimiçi] Available at: https://dsy.usom.gov.tr/usom/23/07/230704142928_Bireysel%20Siber%20Gu%CC%88venlik%20O%CC%88nlemleri.pdf [Erişildi: 10 2 2025].

Verma, A. & Bajaj, S. K. (2008). Cyber Fraud: A Digital Crime. %1 içindeP. I. a. P. P. Miguel Baptista Nunes, dü. *IADIS International Conference Information Systems 2008*. basım yeri bilinmiyor:IADIS Dijital Library, pp. 147-154.

Vodafone, (2025). *Vodafone.* [Çevrimiçi] Available at: https://www.vodafone.com.tr/hakkimizda/zararli-yazilimlar [Erişildi: 10 2 2025].

Yalçınkaya, M. A. & Küçüksille, E. U. (2017). *Uygulamalı Sızma Testleri Pentest Lab.* 4 dü. İstanbul: Abaküs.

Yılmaz, S. & Sağıroğlu, Ş. (2013). *Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri.* Ankara, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.