402 BİLGİSAYAR AĞLARI DERSİ

ARAŞTIRMA ÖDEVİ-III

Ayben GÜLNAR-191180041

MART 2023

İçindekiler Tablosu

Şekiller Listesi

1.GİRİŞ

Teknolojinin gelişmesiyle birlikte internet, hayatımızın her alanına girdi ve artık vazgeçilmez bir hale geldi. İnternet sayesinde, bilgiye anında erişim sağlanabiliyor, iletişim kolaylaşıyor, iş ve öğrenim hayatında farklı olanaklar sunuluyor. Ancak, internetteki hızlı gelişmeler ve yaygın kullanımı, siber güvenlik risklerinin de artmasına neden oldu. Günümüzde, internet ortamında yapılan saldırılar, kişisel verilerin çalınması, ağların çökmesi, bilgisayar korsanlığı gibi birçok zararlı etkiye neden olabilmektedir. Bu nedenle, siber güvenlik konusu günümüzde oldukça önemlidir ve herkesin dikkat etmesi gereken bir konudur.

Şu anda ülkelerin ekonomik, ticari, kültürel ve sosyal aktivitelerinin çoğu, bireyler, sivil toplum kuruluşları dahil olmak üzere tüm seviyelerde, siber uzayda gerçekleştiriliyor. Son zamanlarda, dünya çapında birçok özel şirket ve hükümet kuruluşu siber saldırıların ve kablosuz iletişim teknolojilerinin tehlikesiyle karşı karşıya kalmaktadır. Bugünün dünyası elektronik teknolojiye yüksek derecede bağımlıdır ve bu verileri siber saldırılardan korumak zorlu bir konudur. Siber saldırıların amacı şirketlere maddi zarar vermektedir. Bazı durumlarda, siber saldırılar askeri veya siyasi amaçlar da taşıyabilir. Bu zararların bazıları: PC virüsleri, bilgi çıkarmaları, veri dağıtım hizmeti (DDS) ve diğer saldırı vektörleridir. Bu amaçla, çeşitli kuruluşlar siber saldırıların neden olduğu hasarı önlemek için çeşitli çözümler kullanır. Siber güvenlik, en son BT verilerine ilişkin gerçek zamanlı bilgi takibini izler. Şimdiye kadar dünya genelinde araştırmacılar tarafından siber saldırıları önlemek veya neden oldukları hasarı azaltmak için çeşitli yöntemler önerilmiştir. Bazı yöntemler çalışma aşamasındayken, diğerleri araştırma aşamasındadır [1].

Bu araştırma ödevimin amacı, Internet üzerindeki saldırıları tanımlamak, çeşitlerini detaylıca ele almak ve önlem türlerine göre önlemleri açıklamaktır.

2. INTERNET SALDIRILARI TANIMI VE NEDENLERİ

2.1 Internet Saldırıları Tanımı

Siber saldırı, bilgisayar sistemlerine izinsiz erişim yoluyla bilgi çalmak, açığa çıkarmak, değiştirmek, devre dışı bırakmak veya yok etmek için yapılan istenmeyen girişimlerdir. Virüsler gibi çeşitli yöntemler kullanılarak gerçekleştirilir [2].

2.2. Internet Saldırılarının Gerçekleşme Nedenleri

Cyber suçlarının yanı sıra, siber saldırılar siber savaş veya siber terörizmle de ilişkilendirilebilir, örneğin hacktivistler gibi. Motivasyonlar değişebilir, yani üç ana kategori vardır: suç, siyasi ve kişisel [2].

Suçlu olarak motive olan saldırganlar, para çalma, veri çalma veya işletme bozulması yoluyla maddi kazanç sağlamayı amaçlarlar. Aynı şekilde, memnuniyetsiz mevcut veya eski çalışanlar gibi kişisel olarak motive olanlar, para, veri veya sadece bir şirketin sistemini bozmak için bir fırsat arayabilirler. Ancak, öncelikle intikam almaya çalışırlar. Sosyo-politik olarak motive olan saldırganlar, nedenleri için dikkat çekmeye çalışırlar. Sonuç olarak, saldırılarını halka duyururlar - hacktivism olarak da bilinir. Diğer siber saldırı motivasyonları arasında casusluk, rakiplerine karşı haksız bir avantaj elde etmek için casusluk ve entelektüel zorluk yer alır. Siber saldırılar, işletmelerin, devlet aktörlerinin veya özel kişilerin bir veya birçok şey istemesi nedeniyle meydana gelir, örneğin:

- İşletme finansal verileri
- Müşteri listeleri
- Müşteri finansal verileri
- Kişisel tanımlayıcı bilgileri (PII) içeren müşteri veritabanları
- E-posta adresleri ve giriş kimlikleri
- Ticari sırlar veya ürün tasarımları gibi entelektüel mülkiyet
- Bilgi işlem altyapısı erişimi
- Finansal ödemeleri kabul etmek için IT hizmetleri
- Hassas kişisel veriler [2].

3.INTERET SALDIRILARI TÜRLERİ

3.1 Virüsler ve Solucanlar

Solucanlar, kendi kendine bulaşarak diğer bilgisayarlara enfekte olan bir kötü amaçlı yazılım türüdür ve aktif kalmaya devam eder. İnsan müdahalesi veya bir ana program veya dosya olmaksızın kendini kopyalayabilir. Solucanlar genellikle bir bilgisayar sisteminin işletim sistemindeki açıkları kullanır ve sıklıkla fark edilmeden yayılır.

Saldırganlar solucan kötü amaçlı yazılımı tasarlayarak kurbanın sistemlerine erişim sağlamayı ve yaygın siber suçların yaygın türlerini gerçekleştirmeyi amaçlarlar. Solucanlar dosyaları değiştirebilir, bozabilir, çalabilir ve silebilir, bir makineye ek kötü amaçlı yazılım enjekte edebilir veya sadece sistem kaynaklarını tüketerek bir ağı aşırı yükleyebilir.

Solucan kötü amaçlı yazılım, saldırganların bir kurbanın bilgisayarı üzerinde uzaktan kontrol sağlamak için arka kapılar kurmasına da izin verebilir. Bir kötü amaçlı yazılım solucanı, USB'ler, internet faaliyetleri ve yazılım açıklarından aktarılabilir. Ayrıca spam e-postalarında veya anlık mesajlarda ekler olarak da girebilir. Sistemlere sızdığında, solucan kötü amaçlı yazılımı kötü amaçlı kodu çalıştırırken varlığını gizler. Solucan kötü amaçlı yazılım, verileri değiştirebilir, silebilir veya dışa aktarabilir. Bazı durumlarda, sistem kaynaklarını, örneğin sabit disk alanını tüketmeyi veya paylaşılan bir ağı aşırı yükleyerek operasyonları engellemeyi amaçlar. Genellikle zararsız ve tanıdık bir dosya adı veya bağlantı olarak kamuflaj yaparak görevini yerine getirmesi ve tespit edilmeden aktif kalmaya ve çoğalmaya devam etmesi amaçlanır. Solucanlar, bağımsız ve en yaygın kötü amaçlı yazılım türleri arasındadır. Ancak, farklı türde solucan kötü amaçlı yazılımlara bakalım.

E-posta Solucanları: E-posta solucanları, kullanıcıların listelerindeki tüm kişilere yayılır. Alıcı e-postayı açtığında, kötü amaçlı yürütülebilir dosyaları diğer cihazlara enjekte edebilirler.

Dosya Paylaşımı Solucanları: Bu solucanlar genellikle medya dosyaları olarak kamuflaj yapılır ve özellikle güç istasyonları, su kaynakları kuruluşları gibi endüstriyel ortamlara yönelik hedeflerdir.

Kriptosolucanlar: Kriptosolucanlar, hedef bilgisayardaki verileri şifreleyen ve genellikle bir şifre çözme anahtarı karşılığında fidye talep etmek için kullanılan çok tehlikeli solucanlardır.

İnternet Solucanları: Genellikle internet solucanları, güvenlik sistemleri zayıf veya hiç olmayan popüler web sitelerini hedef alan kötü amaçlı yazılımlardır. Bu siteleri enfekte ederek saldırıları başlatırlar ve zamanla bu sitelere erişen cihazları da enfekte ederler.

Anlık Mesajlaşma Solucanları: Bu tür solucanlar, e-posta solucanları gibi ekler veya bağlantılarla maskelenirler. Tek farkları, e-postalar yerine bir sohbet hizmetinde anlık mesajlar aracılığıyla çalışmalarıdır [3].

3.2 Truva Atları ve Saldırı Yazılımları

Trojan atı, Trojan olarak da bilinen zararlı bir kod veya yazılım türüdür. Sahte görünümde olan bir Trojan, bilgisayarınızın kontrolünü ele geçirebilir. Bir Trojan, verilerinizi veya ağınızı zarar vermek, bozmak, çalmak veya genel olarak başka zararlı eylemler gerçekleştirmek için tasarlanmıştır. Trojan, sizi kandırmak için gerçek bir uygulama veya dosya gibi davranır. Cihazınızda kötü amaçlı yazılımı yüklemeye ve çalıştırmaya sizi inandırmaya çalışır. Yüklendikten sonra, bir Trojan tasarlandığı işlemi gerçekleştirebilir. Bir Trojan bazen Trojan virüsü veya Trojan atı virüsü olarak adlandırılır, ancak bu yanıltıcı bir terimdir. Virüsler kendilerini yürütebilir ve kopyalayabilirler. Bir Trojan ise bunu yapamaz. Kullanıcının Trojana tıklaması gerekir. Bununla birlikte, Trojan kötü amaçlı yazılımı ve Trojan virüsü terimleri

sıklıkla birbirinin yerine kullanılır. En yaygın Trojan malware türlerinden bazıları, isimleri ve bilgisayarınızda yaptıkları şeyler:

Backdoor Trojanı: Bu Trojan, bilgisayarınızda "arka kapı" yaratabilir. Bu sayede saldırgan bilgisayarınıza erişebilir ve kontrol edebilir. Verileriniz üçüncü bir taraf tarafından indirilip çalınabilir. Veya cihazınıza daha fazla kötü amaçlı yazılım yüklenebilir.

Dağıtılmış Hizmet Reddi (DDoS) saldırısı Trojanı: Bu Trojan, DDoS saldırıları gerçekleştirir. Ağın yüksek trafiğe maruz kalarak çökmesi amaçlanır. Bu trafik, sizin enfekte olmuş bilgisayarınızdan ve diğerlerinden gelir.

Downloader Trojan: Bu Trojan, zaten enfekte olan bilgisayarınıza yöneliktir. Yeni kötü amaçlı programların sürümlerini indirir ve yükler. Bunlar Trojanlar ve reklam yazılımlarını içerebilir.

Sahte AV Trojanı: Bu Trojan, antivirüs yazılımı gibi davranır, ancak tehditleri tespit etmek ve kaldırmak için sizden para talep eder, gerçek veya sahte olmalarına bakılmaksızın.

Oyun-hırsızı Trojanı: Kaybedenler burada çevrimiçi oyuncular olabilir. Bu Trojan, hesap bilgilerini çalmaya çalışır.

Infostealer Trojan: Adından da anlaşılacağı gibi, bu Trojan, enfekte olan bilgisayarınızdaki verileri hedefler.

Mailfinder Trojanı: Bu Trojan, cihazınızda biriktirdiğiniz e-posta adreslerini çalmaya çalışır.

Fidye Trojanı: Bu Trojan, bilgisayarınıza verdiği hasarı geri almak için fidye talep eder. Bu, verilerinizi bloke etmek veya bilgisayarınızın performansını bozmak gibi şeyleri içerebilir.

Uzak Erişim Trojanı: Bu Trojan, uzaktan ağ bağlantısı aracılığıyla saldırganlara bilgisayarınız üzerinde tam kontrol sağlayabilir. Kullanım alanları arasında bilgilerinizi çalmak veya sizi izlemek yer alır.

Rootkit Trojanı: Rootkit, enfekte olan bilgisayarınızda bir nesneyi gizlemeyi veya örtbas etmeyi amaçlar. Amacı, kötü amaçlı bir programın cihazınızda çalışma süresini uzatmaktır.

SMS Trojanı: Bu tür Trojan, mobil cihazınızı enfekte eder ve SMS gönderir ve alır. Prim numaralarına gönderilen mesajlar telefon maliyetinizi artırabilir.

Trojan Banker: Bu Trojan, finansal hesaplarınızı hedef alır. Çevrimiçi olarak yaptığınız her şey için hesap bilgilerinizi çalmak [4].

3.3 Phishing Saldırıları

Phishing saldırıları, kullanıcıları yanlış şeyleri yapmaya ikna etmeye çalışan saldırganların yaptığı bir tür saldırıdır. Bu yanlış şeyler arasında kötü amaçlı yazılım indirmeye yönlendiren kötü bir bağlantıya tıklamak veya güvenilmeyen bir web sitesine yönlendirmek yer alır.

Phishing, bir metin mesajı, sosyal medya veya telefondan da gerçekleştirilebilir, ancak terim genellikle e-posta yoluyla gelen saldırıları tanımlamak için kullanılır. Phishing e-postaları, meşru e-postaların yoğunluğu arasında gizlenerek milyonlarca kullanıcıya ulaşabilir. Saldırılar kötü amaçlı yazılımların (örneğin fidye yazılımı) yüklenmesine, sistemleri sabotaj yapmaya veya fikri mülkiyet ve para çalmaya yönelik olabilir.

Phishing e-postaları herhangi bir boyutta ve türdeki bir kuruluşa ulaşabilir. Sizi bir kitlesel kampanyanın parçası yapabilirler (saldırgan sadece yeni şifreler toplamayı veya kolay para kazanmayı amaçlıyorsa) veya şirketinize karşı hedefli bir saldırının ilk adımı olabilirler. Hedefli bir kampanyada, saldırgan, çalışanlarınız veya şirketiniz hakkındaki bilgileri kullanarak mesajlarını daha ikna edici ve gerçekçi hale getirebilir. Buna genellikle olta atma saldırısı denir [5].

3.4 Kimlik Hırsızlığı ve Kişisel Veri Sızıntıları

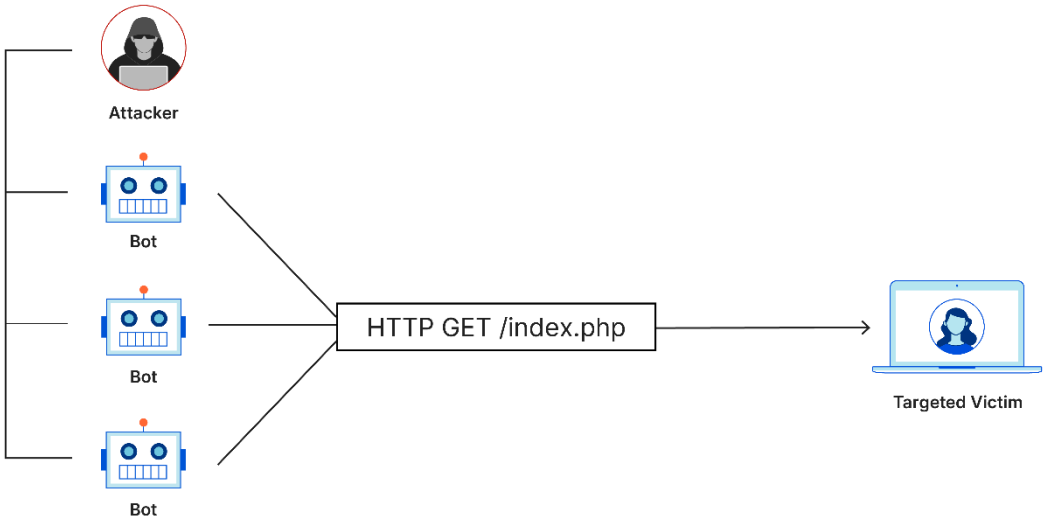
Kişisel bilgilerinizi ele geçirmek için kimlik hırsızlarının kullanabileceği birkaç yöntem vardır. Telefonla kredi kartı numaranızı okurken dinlemek, bir veri ihlalinde açığa çıktıktan sonra karanlık web'de satın almak veya benzersiz bir yöntem kullanmak gibi. Kimlik hırsızlığı süreci daha sonra bu verileri kullanma aşamasına geçer.

Finansal kimlik hırsızlığı: Bu tür suç faaliyetini, özel verileri finansal hesaplara erişmek için kullanmakla ilişkilendiren çoğu insan kimlik hırsızlığı olarak düşünür. Kredi kartı veya banka hesap özeti herhangi bir anormal hareket gösterirse, üç kredi raporu şirketini ayrı ayrı arayarak kredi raporlarınıza 90 günlük bir dolandırıcılık uyarısı koymalı ve hesabı olan her finansal kuruluşla iletişime geçmelisiniz.

Suç kimliği hırsızlığı: Suç kimliği hırsızlığı, suçlama veya tutuklanma durumunda, bir başkasının adını ve diğer kişisel bilgilerini kullanarak kişiyi taklit etmek anlamına gelir. Mağdur, suçun çok geç olana kadar farkına varmayabilir ve artık adı altında bir suç kaydı bulunabilir. Suç kimliği hırsızının gerçek veya sahte fotoğraf kimliği ve ad, sürücü ehliyeti numarası veya Sosyal Güvenlik numarası gibi bilgileri kullanması mümkündür [6].

3.5 DDoS Saldırıları

Dağıtık hizmet reddi saldırısı (DDoS), bir hedef sunucu, hizmet veya ağı normal trafiğini bir internet trafiği seli ile engelleyerek hedefi veya çevre altyapısını bozmaya yönelik kötü niyetli bir girişimdir. DDoS saldırıları, saldırı trafiği kaynağı olarak birden fazla ele geçirilmiş bilgisayar sistemi kullanarak etkililik elde eder. Saldırıya maruz kalan makineler arasında bilgisayarlar ve IoT cihazları gibi diğer ağ kaynakları da olabilir. Yüksek düzeyde bakıldığında, DDoS saldırısı, beklenmedik bir trafik tıkanıklığı olarak düşünülebilir ve düzenli trafiğin hedefine ulaşmasını engeller. DDoS saldırıları, internet bağlantısı olan makinelerin ağları ile gerçekleştirilir. Bu ağlar, kötü amaçlı yazılımlarla enfekte edilmiş bilgisayarlar ve IoT cihazları gibi diğer ağ kaynaklarından oluşur. Bu bireysel cihazlar, bir saldırgan tarafından uzaktan kontrol edilebilmeleri için kötü amaçlı yazılımlarla enfekte edilmiştir. Bu cihazlar zombiler ya da botlar olarak adlandırılır ve bir grup bot, botnet olarak adlandırılır. Bir botnet oluşturulduktan sonra, saldırgan her bir bota uzaktan talimatlar göndererek bir saldırı yönlendirebilir. Kurbanın sunucusu veya ağı botnet tarafından hedef alındığında, her bot hedefin IP adresine istek göndererek sunucunun veya ağın normal trafikten engellenmesine neden olabilir. Her bir botun gerçek bir internet cihazı olması nedeniyle, saldırı trafiğini normal trafiğinden ayırmak zor olabilir.



Şekil 3.5.1 Application Layer Attack

Farklı DDoS saldırı türleri, bir ağ bağlantısının çeşitli bileşenlerine yönelik hedeflemelerde bulunurlar. Farklı DDoS saldırılarının nasıl çalıştığını anlamak için, bir ağ bağlantısının nasıl yapıldığını bilmek gereklidir. İnternet'teki bir ağ bağlantısı, birçok farklı bileşen veya

"katman"dan oluşur. Bir evi yere temelden inşa etmek gibi, modeldeki her katmanın farklı bir amacı vardır. Aşağıda gösterilen OSI modeli, ağ bağlantısını 7 ayrı katmanda açıklamak için kullanılan bir kavramsal çerçevedir [7].

4.INTERNET SALDIRILARINA KARŞI KORUNMA YÖNTEMLERİ

İnterneti kullanırken virüslerden ve solucanlardan kendinizi ve ailenizi korumak için bazı temel kurallara uymak önemlidir. İlk olarak, ileri düzey saldırılara karşı koruma sağlayan anti-virüs, güvenlik duvarı ve anti-phishing teknolojileri sunan McAfee Total Protection gibi güçlü ve güncel güvenlik yazılımı kullanın. Ayrıca, güçlü anti-spam ve anti-phishing prosedürleri uygulayan bir internet servis sağlayıcısı seçin ve işletim sisteminiz ve diğer yazılımlar için düzenli olarak güncellemeler yükleyin. Ek olarak, ekler açılırken dikkatli olun, belirli dosya uzantılarını indirmekten kaçının ve mobil telefonlar da dahil olmak üzere tüm cihazlarda güvenlik önlemleri kullanın. Spam tabanlı phishing dolandırıcılıklarına dikkat edin ve anlık mesajlaşma uygulamanızı doğru şekilde yapılandırın. Son olarak, dosyalarınızı düzenli olarak yedekleyin ve önemli bilgileri geri yükleyebilmek için bunları kişisel bilgisayarınızın dışında saklayın, böylece bir virüs saldırısına maruz kalırsanız bile önemli bilgilerinizi kurtarabilirsiniz. Bir önemli tedbir, kahve dükkanları, havaalanları veya oteller gibi halka açık Wi-Fi ağlarını kullanırken dikkatli olmaktır. Bu ağlar genellikle güvenli değildir ve hackerların kolayca istismar etmesine olanak sağlar. Kendinizi korumak için internet trafiğinizi şifrelemek ve çevrimiçi etkinliğinizi gizli tutmak için sanal özel ağ (VPN) kullanmayı düşünebilirsiniz. Başka bir önemli adım, ziyaret ettiğiniz web siteleri ve tıkladığınız bağlantılara dikkat etmektir. Siber suçlular sıklıkla kişileri şifreler veya kredi kartı numaraları gibi kişisel bilgiler sağlamaya ikna etmek için phishing dolandırıcılığı kullanırlar. Bu dolandırıcılıklara düşmemek için, hassas bilgi isteyen istenmeyen e-postalardan veya mesajlardan kaçının ve giriş kimlik bilgilerinizi girerken herhangi bir web sitesinin URL'sini çift kontrol edin. Ayrıca, sosyal medya platformları ve diğer web sitelerindeki gizlilik ayarlarınızı düzenli olarak gözden geçirmek iyi bir fikirdir. Kişisel bilgilerinizi paylaşma miktarını sınırlamak için ayarlarınızı ayarlamak, kimlik hırsızlığı veya diğer siber suçların riskini azaltmaya yardımcı olabilir [8].

Cyber-suçluların teşhis edilmekten kaçınmak için daha sofistike hale geldiği ve birçok modern kötü amaçlı yazılım aracının antivirüs ve diğer tehdit tespit önlemlerini atlatmak için yeni yollar benimsemeye başladığı bilinmektedir. Ağlar ve organizasyonlar saldırıları tespit etmek ve yanıtlamak için sofistike yöntemler kullanıyor, bu da suçluların daha güçlü bir şeyle yanıt vermeye çalışmasına neden oluyor. Siber suçluların karmaşıklığı artıyor ve yapay zeka (AI) saldırıları için genişleyen potansiyel ile birleşiyor.

Ancak siber güvenlik kritik bir kavşakta ve alan gelecekteki araştırma çabalarını savunma çözümlerine dayanmak yerine kritik senaryoları ve sonuçları önceden tahmin edebilen siber saldırı öngörü sistemlerine odaklamalıdır. Dünya genelindeki bilgisayar sistemleri, siber tehditlerin kapsamlı, öngörüsel bir analizine dayalı sistemlere ihtiyaç duyar. Özellikle makine öğrenmesine (ML) yoğun şekilde dayanan yapay zeka (AI), geçmiş deneyimlerden ortaya çıkan desenleri tanıma ve buna dayanarak tahminler yapma yeteneğine sahiptir. Son yıllarda, makine öğrenmesi ve yapay zeka gibi şeyleri kullanarak ağlara ve cihazlara saldırmak için kullanılabilen sürü teknolojisi yeni bir potansiyel göstermiştir. Saldırı desenlerinin farkına vararak kullanışlı saldırı desenleri, kötü amaçlı faaliyetler arasındaki desen ve bağlantıları analiz ederek gelecekteki hamleleri tahmin ederek potansiyel olarak kötü amaçlı davranışları önlemek veya tespit etmek mümkündür.

Yukarıda bahsedilen siber tehdit öngörü sistemleri umut verici ve sınırlı olanaklar sunsa da, büyük ölçekli koordineli saldırılar, bilgisayar sistemlerinde oluşturulan olayların tespiti ve tahmin edilmesi gibi birkaç önemli noktada ilerleme gerektirir. Ağın tespit edilmesini atlatmak için kasıtlı olarak kötü amaçlı kodu anlaşılması zor hale getiren bulanıklaştırma teknikleri kullanılır. Yapay zeka (YZ), özellikle makine öğrenimine (MO) ağırlık veren, geçmiş deneyimlerden ortaya çıkan desenleri tanıma ve bunlara dayanarak tahminler yapma yeteneğine sahiptir. Son yıllarda, makine öğrenimi ve yapay zekayı kullanarak ağları ve cihazları hedef alabilen sürü teknolojisi de yeni potansiyel göstermiştir.

Kullanışlı saldırı modelleri, kötü amaçlı etkinlikler arasındaki bağlantıları ve desenleri analiz ederek, gelecekteki hamleleri tahmin ederek ve sonunda potansiyel olarak kötü amaçlı davranışları önleyerek veya tespit ederek tanımlanabilir.

Yukarıda bahsedilen siber tehdit tahmin sistemleri umut verici ve sınırlı olasılıklar sunarken, büyük ölçekli koordineli saldırılar, bilgisayar sistemlerinde üretilen olayların tespiti ve tahmini gibi birkaç alanda ilerleme gerektirir. Ağın tespiti engellemek için kötü amaçlı kodları anlamakta kasıtlı olarak zorlaştırmak için obskürizasyon teknikleri kullanılır.

Ağ güvenliği riskleri değerlendirilirken, hackerların davranışı göz önünde bulundurulmalıdır, çünkü bir ağa sızmak için seçebilecekleri bilinen açıkların sayısı ve seçenekleri göz korkutucu bir görev olabilir. Özellikle siber saldırıları tanımlamak için veri, bilgisayar ve ağ saldırılarını karakterize etmek için iki derin öğrenme teknikleri kullanılmıştır. Ayrıca, bilgi teorisi temelli ayrıklaşma ölçüleri entegre edilerek olası bilgisayar ve ağ saldırıları oluşturulur ve düzenlenir.

Başka bir proje olan ASSERT/CASCADES, siber suçluların sürekli değişen teknikleri hakkında daha fazla bilgi edindikçe gelişmektedir. Bu proje, ağda gözlemlenen kötü amaçlı etkinlikleri kullanarak yaklaşan saldırıları tahmin etme yeteneğine sahiptir. Bu sayede kritik tehditler önceden tespit edilerek, devam eden kötü amaçlı etkinliklerden farklı stratejiler geliştirilebilir ve önlem alınabilir. Bahsedilen siber tehdit tahmin sistemleri umut verici ve sınırlı olasılıklar sunsa da, büyük ölçekli koordineli saldırılar, bilgisayar sistemlerinde üretilen olayların tespiti ve tahmini de dahil olmak üzere birçok önemli alanda ilerleme gerektirmektedir. Ağ güvenliği riskleri değerlendirilirken, hacker'ların davranışı da dikkate alınmalıdır ki bu, bir ağa sızmak için yapabilecekleri seçimler ve bilinen zayıflıkların sayısı göz önüne alındığında, zorlu bir görev olabilir [9].

4.1 Data Science ile Güvenlik Önlemi

Cyber security ve veri bilimi, hacker'larla mücadele etmek için yaygın olarak kullanılır. Bu tür çalışmaların bir adı bile var: CSDS (cyber security data science). CSDS hala oldukça yeni ve gelişme için birçok fırsat var. Bazı zorluklar şunları içerir:

Cyber security tehditlerinin değişken doğası. Hacker'lar sürekli olarak olası zayıf noktaları geliştirip sömürdükleri için, bu tehditleri azaltmak için yeni veri bilimi yaklaşımları dinamik olmalıdır. Veri bilimindeki ilerlemelerin, hacker endüstrisine de yarar sağladığını unutmayın. Aradığınız şeyi biliyorlarsa, tespit edilmekten kaçınmak daha mümkündür. Temel oran yanılgısı ve temel oran ihmal ediliyor. Cyber security ve dolandırıcılık tespitinde en az %90 vakalar normal olacak ve şüpheli aktivite nadir olacaktır. Bir algoritmanın tahmin doğruluğu, başarı ölçüsü olarak etkili bir ölçüt değildir. Bunun yerine, bu tür sorunlar genellikle aykırı değer tespiti tekniklerini gerektirir. Sınıflandırma hatalarının asimetrik maliyetleri. Cyber security'de bir saldırıyı kaçırmak, faaliyeti yanlışlıkla şüpheli olarak etiketlemekten daha yüksek maliyetli olabilir. İnsan uzmanının yanlış pozitifler üzerine daha fazla araştırması, onu yanlış olarak gösterebilir. Ancak, bir saldırıyı yanlış negatif olarak kaçırmak, bir kuruluş üzerinde yıkıcı etkilere sahip olabilir. Bu anlamda, veri biliminin cyber security'ye uygulanması, veri biliminin tıbba uygulanmasına benzer.

Veri Bilimcisinin Cyber Security'ye yönelik bazı zorlukları tartışmaktadır. CSDS alanındaki en büyük sorunlardan biri, eğitim için iyi veri kümelerinin eksikliğidir. Cyber security saldırılarından kaçınmaya çalışan şirketlerin verilerini paylaşmayacakları kolayca anlaşılabilir [10].

5. SİBER SALDIRILARDA YASA VE YÖNETMELİKLER

5809 sayılı Elektronik Haberleşme Kanunu'na 2014 yılında eklenen Ek Madde 1 ile Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. USOM, siber güvenliğe yönelik ulusal ve uluslararası çalışmalar yapmakta, tehditleri belirleyerek müdahale etmek için ilgili aktörlerle koordinasyon sağlamaktadır. Ayrıca Siber Olaylara Müdahale Ekipleri (SOME) kurularak, Bakanlıklar bünyesinde siber saldırılara karşı önlemler almak ve müdahale etmekle yükümlü birimler oluşturulmuştur. Kişisel verilerin korunması için ise 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Kişisel Verileri Koruma Kurumu kurulmuştur. Bu kurum, kişisel verilerin işlenmesindeki usul ve esasları düzenlemektedir [11].

7.SONUÇ

Sonuç olarak, günümüzde siber suçluların taktikleri ve araçları giderek daha sofistike hale gelmektedir ve bu durum siber güvenlik uzmanlarının siber saldırıların önceden tahmin edilebilmesi için daha kapsamlı ve öngörülü çözümler geliştirmesi gerektiği anlamına gelmektedir. Makine öğrenimi ve yapay zeka tekniklerinin kullanılması, saldırgan davranışlarının analiz edilmesi, gelecekteki saldırılarının tahmini ve bu saldırıların tespit edilmesi için yeni yollar sunmaktadır.

Kaynaklarda bahsedilen birçok araştırma projesi, siber güvenlik risklerini önceden tahmin etmek için farklı yöntemler önermektedir. Örneğin, gözlemlenen kötü niyetli faaliyetleri kullanarak saldırıların önceden tahmin edilebilmesine yardımcı olan ASSERT/CASCADES projesi, siber saldırılarının modellenmesi için yenilenmiş suç teorilerini kullanmaktadır. NEPAR projesi ise 1.5 milyondan fazla siber saldırı örneğinden veri toplamış ve her saldırının karakteristik özelliklerini ve kullanılan desenleri analiz ederek, belirli sistemlere yönelik olası saldırı olasılıklarını tahmin etmiştir.

Bununla birlikte, siber güvenlik her zaman bir savunma savaşı olarak kalacaktır ve tüm saldırıları önceden tahmin etmek imkansızdır. Bu nedenle, işletmelerin siber güvenlik önlemlerini artırmaları, güvenlik açıklarını sürekli olarak tarayarak düzenli olarak güncelleme yapmaları ve çalışanlarına siber güvenlik eğitimi vererek, siber saldırılara karşı daha hazırlıklı olmaları gerekmektedir. Ayrıca, siber güvenlik uzmanlarına da yeni tehditleri önceden tahmin etmek ve savunmaya hazırlanmak için gelişen teknolojileri yakından takip etmeleri önemlidir.

Sonuç olarak, siber saldırılara karşı korunmak, tüm sektörler için önemli bir konudur ve siber güvenlik teknolojileri ve stratejileri sürekli olarak geliştirilmelidir. İşletmelerin, siber güvenlik uzmanlarına ve teknolojilere yatırım yapmaları ve siber güvenlik konusunda bilinçli olmaları gerekmektedir.

8.KAYNAKÇA

[1]Elif, S., Ozturk, M. E., & Sahin, O. (2022). A Comprehensive Review on Cyber Security: Advancements, Challenges and Future Directions. Journal of King Saud University - Computer and Information Sciences, 34(2), 101523. https://doi.org/10.1016/j.jksuci.2021.101523

[2]IBM. (Erişim tarihi: 28 Mart 2023). Cyberattack. https://www.ibm.com/topics/cyber-attack

[3]EasyDMARC. (2021, March 31). What is a Computer Worm and How Does it Work? Retrieved from https://easydmarc.com/blog/what-is-a-computer-worm-and-how-does-it-work/

[4]Norton. (n.d.). What Is a Trojan? Retrieved March 28, 2023, from https://us.norton.com/blog/malware/what-is-a-trojan [5] Ma, W., Liu, J., & Liu, K. (2001).

[5]National Cyber Security Centre (NCSC). (2021). Phishing. https://www.ncsc.gov.uk/guidance/phishing

[6]Maaz, M. (2022, December 6). Identity Theft & Cybersecurity Measures. Dataconomy. https://dataconomy.com/2022/12/identity-theft-cybersecurity-measures/

[7]Cloudflare. (n.d.). What is a DDoS attack? Cloudflare. Retrieved March 28, 2023, from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[8]Bilgisayarınızı Virüs ve Solucan Saldırılarından Koruma Yolları.Türk Telekom Güvenlik, https://turktelekomguvenlik.com/bireysel/guvenlik-onerileri/bilgisayarinizi-virus-ve-solucan-saldirilardan-koruma-yollari. Erişim tarihi: 28 Mart 2023.

[9]Sahoo, S. K., Lenka, R. K., & Patel, A. K. (2019). Predictive analysis of cyber security threats using machine learning algorithms. International Journal of Emerging Trends in Engineering Research, 7(5), 2355-2360.

[10]Salleh, R. (2021). Using Data Science to Find Cyber Security Threats. Geek Culture. https://medium.com/geekculture/using-data-science-to-find-cyber-security-threats-75c02c2068ea

[11]Bilgem TÜBİTAK. (t.y.). Siber Güvenlik Mevzuatı. Dijital Akademi. https://dijitalakademi.bilgem.tubitak.gov.tr/siber-guvenlik-mevzuati/