J. Innovative Eng. Nat. Sci., c. 4, s. 1, ss. 113-125, 2024.
http://doi.org/10.61112/jiens.1380821

JIENS
Journal of Innovative Engineering and Natural Science
(Yenilikçi Mühendislik ve Doğa Bilimleri Dergisi)
journal homepage: https://jiens.org

Araştırma Makalesi

Siber ağların risk analizi: Saldırı-savunma ağaçlarıyla temellendirilmiş niceliksel bir yaklaşım

Mehmet Ertem[a,*] ve İlker Özçelik[b]

[a]Endüstri Mühendisliği Bölümü, Eskişehir Osmangazi Üniversitesi, Meşelik Kampüsü, Eskisşehir26040, Türkiye.
[b]Yazılım Mühendisliği Bölümü, Eskişehir Osmangazi Üniversitesi, Meşelik Kampüsü, Eskisşehir26040, Türkiye.

MAKELE BİLGİSİ

Makale Geçmişi:
Geliş 25 Ekim 2023
Düzeltme 27 Kasım 2023
Kabul 14 Aralık 2023

Çevrimiçi mevcut

Anahtar Kelimeler:
Siber güvenlik risk analizi
Saldırı savunma ağacı
Siber risk yönetimi
Eniyi kaynak tahsisi

ÖZET

Günümüzde siber saldırıların ve potansiyel zararlarının hızla artmasıyla birlikte, şirketler ve kurumlar için siber güvenliğin sağlanması hayati bir öneme sahip hale gelmiştir. Bu çalışmada, siber risklerin nicel bir analizi için saldırı-savunma ağaçları tabanlı bir yaklaşım geliştirilmiştir. Önerilen yaklaşım, siber tehditleri temsil eden düğümlerin risk seviyelerini ölçerek toplam riski hesaplamak için saldırı-savunma ağacını kullanmaktadır. Ayrıca, belirlenen savunma önlemlerinin alınması durumunda güncellenmiş risk değerini sistematik bir şekilde hesaplamaktadır. Geliştirilen siber risk analizi yaklaşımı, oltalama saldırılarına yönelik yaygın bir senaryoya uygulanmış ve çeşitli savunma stratejileri altında siber risk değerleri hesaplanmıştır. Örneğin, savunma önlemleri alınmadığı durumda siber risk değeri 0,28392 olarak hesaplanırken, teknik savunma önlemlerinin (antivirüs, IDS, erişim denetimi, web içerik sınırlandırma ve spam kontrolü) alınması durumunda risk değeri yaklaşık %97,5 azalarak 0,00721 seviyesine düşmektedir. Teknik savunma önlemlerine ek olarak kullanıcı eğitimi de verildiğinde risk değerindeki azalma %98'e ulaşmaktadır. Sadece bireysel kullanıcılara yönelik temel savunma önlemlerinin (antivirüs ve spam kontrolü) alınması durumunda risk değerindeki azalma ise %90 civarında kalmaktadır. Örnek çalışma üzerinden elde edilen bu sonuçlar, önerilen yaklaşımın doğruluğunu ve önemini kanıtlamaktadır. Geliştirilen yaklaşımın siber güvenlik stratejilerinin belirlenmesi yolunda katkıları tartışma bölümünde detaylandırılmıştır.

Risk analysis of cyber networks: a quantitative approach based on attack-defense trees

ARTICLE INFO

Article history:
Received 25 Sep 2023
Received in revised form 27 Nov 2023
Accepted 14 Dec 2023

Available online

Keywords:
Cybersecurity risk analysis
Attack defense tree
Cyber risk management
Optimal resource allocation

ABSTRACT

With the rapid increase in cyber-attacks and potential damage in today's world, ensuring cybersecurity has become of paramount importance for companies and organizations. In this study, an approach based on attack-defense trees has been developed for the quantitative analysis of cyber risks. The proposed methodology utilizes attack-defense trees to measure the risk levels of nodes representing cyber threats and systematically calculate the total risk when specific defense measures are implemented. The developed cyber risk analysis approach has been applied to a common scenario involving phishing attacks, and cyber risk values have been calculated under various defense strategies. For instance, when no defense measures are taken, the cyber risk value is calculated as 0.28392. However, when technical defense measures such as antivirus software, intrusion detection systems (IDS), access control, web content filtering, and spam control are implemented, the risk value significantly decreases by approximately 97.5% to 0.00721. Furthermore, incorporating user training results in a 98% reduction in risk value. Implementing basic defense measures targeting individual users, such as antivirus and spam control, leads to a reduction of around 90% in the risk value. The accuracy and significance of the proposed approach are demonstrated through the results obtained from this sample study. The contributions of the developed approach to determining cybersecurity strategies are detailed in the discussion section.

*Sorumlu yazar. Tel.: +90-544-367-3441; e-mail: mertem@ogu.edu.tr

I. GİRİŞ

Verilerin sürekli olarak dijital ağlar boyunca akış halinde olduğu bağlantılı bir dünyada siber güvenlik her geçen gün çok daha önemli hale gelmektedir. Siber tehditler, kötü niyetli kişilerce (hacker) kurumların ve kuruluşların zayıf noktalarını kullanarak savunmalarını aşma çabaları için giderek daha sofistike taktiklerin uygulandığı bir hale evrilmektedir. Kuruluşlar, dijital varlıklarını ve hassas bilgilerini koruma konusundaki çabalarını artırırken, sağlam ve veri odaklı siber risk değerlendirme metotlarına olan ihtiyaç kritik hale gelmiştir. Siber risk konusunda kabul görmüş tanım ve terimlerin henüz oluşmaması sebebiyle siber riski tanımlama [1], etkileyen faktörleri belirleme [2] ve sektörel etkilerini inceleme [3] üzerine çalışmalar yapılmaya başlanmıştır. Öte yandan siber risk alanında yeterli veri setinin bulunmamasının etkileri ve bu konudaki çözüm önerileri Cremer vd. [4] tarafından 2022 yılında yayınlanmıştır. Ayrıca Eling vd. [5] siber riski kurumsal risk yönetim süreçlerine dahil etmenin önemli ve disiplinler arası çalışma gerektiren zor bir problem olduğunu vurgulamıştır.

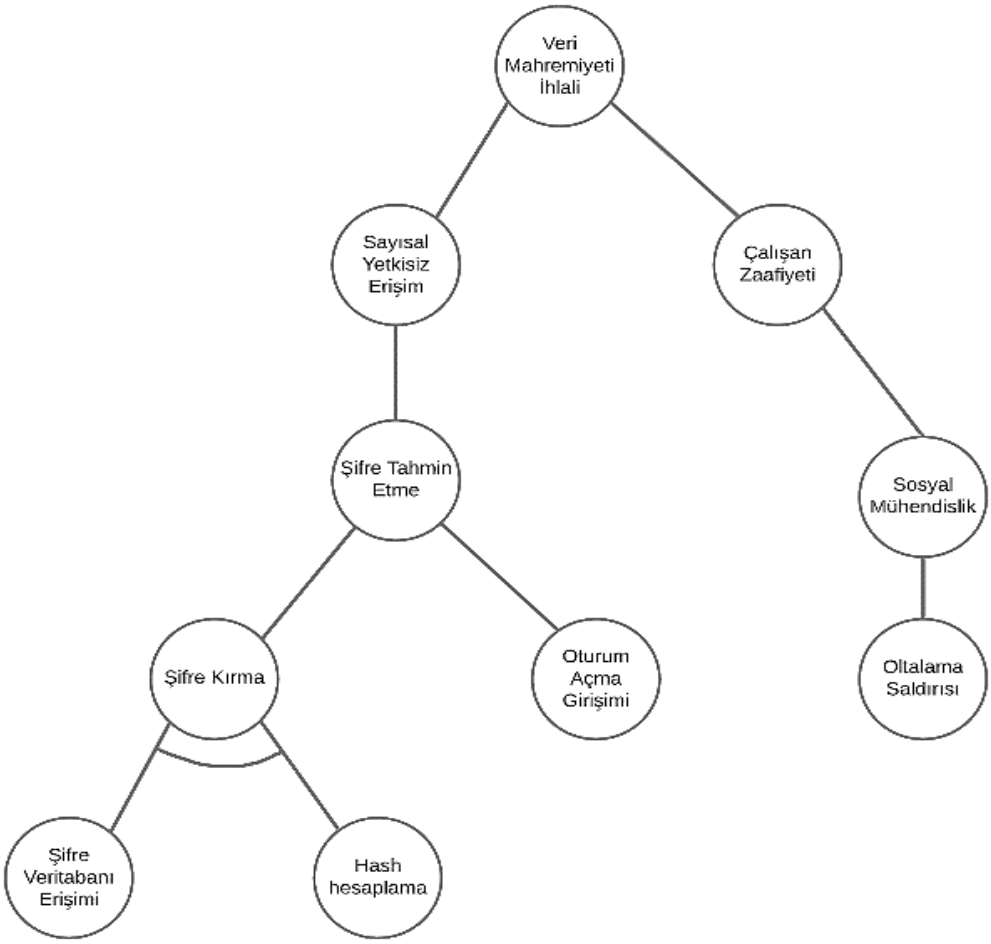
Son yıllarda popülerlik kazanan bu metodolojilerden biri de saldırı ağaçlarını nicel siber risk değerlendirmesi için kullanmaktır. Saldırı ağaçları, siber güvenlik profesyonellerinin kullandığı güçlü bir araç olup potansiyel siber tehditleri modelleme ve analiz etmek için yapılandırılmış ve sistematik bir yaklaşım sunar. Bu grafiksel temsilciler, kuruluşların karmaşık saldırı senaryolarını yönetilebilir bileşenlere bölmelerine yardımcı olarak, kötü niyetli aktörlerin kullanabileceği karmaşık zayıf noktaların ve saldırı yollarının iç içe geçmiş ağına ışık tutar. Saldırı ağaçları uzun süredir nitel tehdit analizi için kullanılmış olsa da nicel risk analizine uygulanması daha yeni bir alan olup büyük potansiyele sahiptir.

Bu makale, saldırı-savunma ağaçlarını kullanan bir nicel siber risk analizi yaklaşımı geliştirerek kuruluşların risk durumlarını daha derinlemesine anlamak için bu metodolojiyi nasıl kullanabileceklerini açıklamaktadır. Geliştirilen model, saldırı-savunma ağacı öğelerine çeşitli olasılıklar ve sonuçlar atayarak siber tehditlerin olasılığını ve etkisini hesaplama yoluyla bilinçli karar verme, kaynak tahsis etme ve risk azaltma stratejilerinin geliştirilmesinde kuruluşlara yol göstermeyi hedeflemektedir. Ayrıca, saldırı-savunma ağaçlarını nicel bir çerçeveye entegre etmek, kuruluşların güvenlik önlemlerini etkili bir şekilde önceliklendirmelerine ve siber güvenlik yatırımlarını optimize etmelerine olanak tanır.

Bilgisayar ağlarının güvenliği için birçok çözüm yaklaşımı geliştirilmiştir. Bununla birlikte, çoğu geleneksel ağ güvenliği çözümü, nicel bir karar verme sürecinden yoksundur. İdeal olarak, böyle bir çerçeve saldırganın davranışlarını dikkate almalıdır. Bu doğrultuda geliştirilen saldırı ağaçları literatürde geçen en yaygın siber güvenlik analizi araçlarından biridir. Bir saldırı ağacı esasen "bir bilgisayar ağına saldırmak için olası tüm senaryoların özlü ve eksiksiz bir temsilidir" [6]. Başka bir deyişle, kaynak düğümden (bilgisayar sistemine ilk giriş noktası) uç düğüme (sistemin başarılı bir şekilde ele geçirilmesi) bir yol üzerindeki her ark, saldırgan tarafından gerçekleştirilebilecek bir eylemi temsil eder (örneğin, parola kırma, belirli bir sunucuya yönetici erişimi, istenen veri tabanına başarılı erişim vb.). Saldırı ağaçlarını kullanarak, optimal veya optimale yakın savunma stratejileri belirlemek mümkündür.

Şekil 1'de bir kurumda gerçekleşebilecek veri mahremiyeti ihlali saldırılarını gösteren basitleştirilmiş bir saldırı ağacı sunulmuştur. Saldırı ağacında düğümler bir saldırı senaryosunu oluşturan birim saldırıları ve kenarlar saldırılar arasındaki ilişkiyi gösterir [7]. Ağacın en üstündeki düğüm, saldırının hedefini temsil eden kök düğümdür. Kök düğümden başlayıp takip eden tüm düğümler kendisini oluşturan alt birim saldırıları temsil eden çocuk düğümler ile gösterilir. Eğer bir düğümün çocuk düğümü yok ise ilgili düğüm dahil olduğu yol üzerindeki

saldırıyı gerçekleştirmek için gerekli gözlenebilen en temel saldırı birimini temsil eder. Bir saldırı senaryosunda, alt birim saldırılar bir yay ile birleştirilmişse, hedef saldırının gerçekleşmesi için bağlı tüm saldırıların gerçekleşmesi gerekir. Sistemi kök düğümde belirtilen saldırıya karşı koruyan savunmacı, bu saldırı ağacını kullanarak saldırı yüzeyini belirleyip bütçesine bağlı olarak en uygun savunma yöntemini seçebilir.



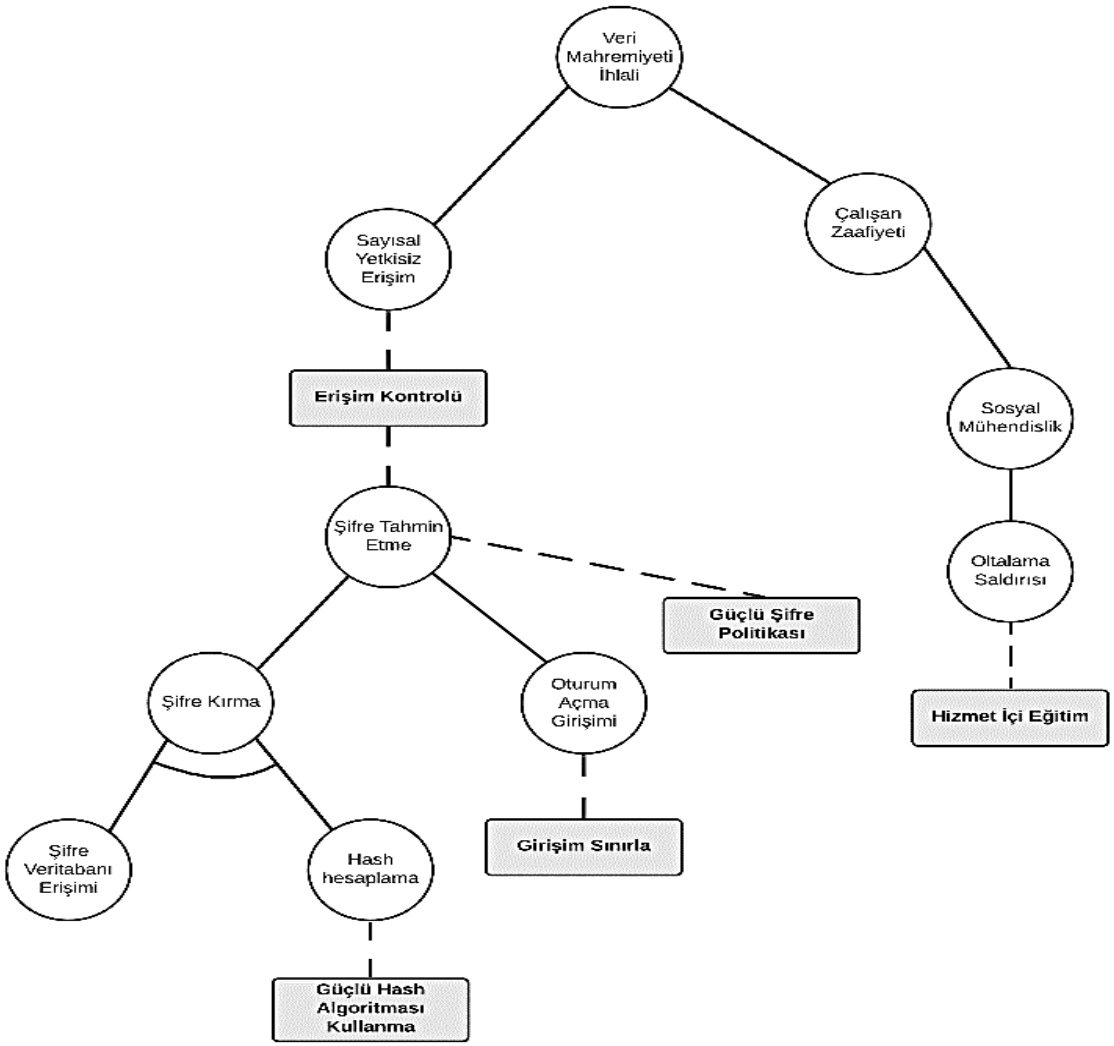
Şekil 1. Saldırı ağacı örneği

Saldırı ağaçları saldırganın hedefe ulaşabilmesi için kullanabileceği farklı yolları gösteren ve sistem güvenliğini olası saldırıların bir fonksiyonu olarak tanımlayan formal bir yöntemdir [7]. Ancak, saldırı ağaçları bir saldırıya karşı gerçekleştirilmiş savunma yaklaşımlarının etkisini ve saldırgan veya savunmacının sisteme müdahaleleri sonrası sistem güvenlik evrimini göstermez [8].

Saldırı Savunma Ağaçları, saldırı ağaçlarının bu eksikliğini tamamlayarak saldırgan ve savunmacının hamlelerini temsil edebilmek için 2 tür (saldırı ve savunma) düğüm kullanımını mümkün kılar. Bu sayede saldırganın ve savunmacının hamlelerinin etkinliği analiz edilebilir [8]. Saldırı Savunma Ağaçlarında birbirine karşı çalışan iki düğüm türü olduğu için düğümler arası ilişkiler düzeltme ve önlem geçişleri ile temsil edilir. Kök düğümünde saldırı ile başlayan bir ağaçta düzeltmeler ilgili düğümü alt birim saldırı düğümlerine bağlarken, önlem geçişleri ilgili düğüme karşı gerçekleştirilen düğümler ile bağlantıyı sağlar.

Basit bir Saldırı Savunma Ağacı örneği Şekil 2'de verilmiştir. Şekil 1'de verilen veri mahremiyet saldırı ağacına savunmacının hamleleri eklenerek saldırı savunma ağacı oluşturulmuştur. Ağaçta aynı türden eylemler (düzeltmeler) düz, birbirine karşı eylemler (önlem) kesikli çizgi ile gösterilmiştir. Yukarıda verilen ağaç eksiksiz bir ağaç olmayıp, olası diğer saldırı ve savunma vektörleri eklenerek kolaylıkla güncellenebilir.

Saldırı Savunma Ağaçlarında senaryolar düğümlerdeki önlem ve düzeltme eylem çiftleri olarak tanımlanır. Bir senaryonun gerçekleşmesi için ilgili düzeltmeler gerçekleştirilirken önlemlerin gerçekleşmemesi gerekir [9]. Şekil 2`deki ağaçta sayısal yetkisiz erişimin sağlanması için savunmacı güçlü şifre politikası uygulamazken, saldırganın başarılı bir şifre tahmin etme saldırısı gerçekleştirmesi gerekir. Saldırı Savunma Ağaçları gerekli matematiksel denklemler tanımlanıp farklı amaçlar için (saldırının en az maliyeti, uygulanan savunmanın etkisi vb.) senaryolar yardımı ile analiz edilebilir [9]. Saldırı savunma ağaçlarının gerçek hayat uygulaması ve bu ağaçları kullanarak RFID-tabanlı ürün yönetimi sistemlerine gerçekleştirilebilecek hizmet engelleme saldırılarına karşı zafiyet senaryolarının nitel analizi Bagnato vd. [10] tarafından yapılmıştır. Saldırı ve savunma ağaçlarını kullanarak siber güvenlik analizi ve risk değerlendirme çalışmaları son yıllarda tekrar hız kazanmaya başlamıştır.



Şekil 2. Saldırı savunma ağacı örneği

He vd. [11] endüstriyel kontrol sistemleri güvenlik değerlendirmesi için saldırı savunma ağaçlarını kullanmıştır. Bu çalışmada yazarlar havaalanı yakıt tedarik sistemi otomasyonunun risk değerlendirmesini Fuzzy Analitik Hiyerarşik Süreç ve saldırı- savunma ağacı kullanılarak gerçekleştirmiştir. Rios vd. [12] saldırı- savunma ağaçlarını kullanarak akıllı şebekelerde kullanılabilecek bir risk değerlendirme metodolojisi önermiştir. Önerilen yöntem akıllı saldırgan ve akıllı savunmacı hamlelerini göz önünde bulunduran ve olası hamlelerin güncellenmesi sonrası risk değerini güncelleyen bir yapıda tasarlanmıştır. Guo vd. [13] bir alfa ayrışma ölçüsü geliştirip bu ölçüyü değişken ağırlık tabanlı siber risk değerlendirme yöntemi geliştirmek için kullanmıştır. Yazarlar ayrışma ölçütünü saldırı- savunma ağacındaki farklı saldırı yollarının risk ağırlıklandırmasında kullanmıştır. Hyder vd [14] CySec Game isminde Siber Fiziksel Sistemler ve Kritik Altyapılar için siber risk değerlendirmesinde kullanılabilecek bir çerçeve sistem ve yazılım önermiştir. Sistem tasarımında saldırı ağaçları, saldırı- savunma ağaçları ve oyun teorisi kullanılmış ve sistemin siber risk değerlendirme amaçlı kullanımının yanı sıra riski incelenen sistemde yüksek riskli hedeflerin belirlenmesi ve savunma harcaması optimizasyonu amaçlı kullanılabileceği belirtilmiştir.

Mondal vd. [15] E-devlet portallarının gereksinimlerini inceleyip güvenlik parametrelerini ölçmek için yöntem önermiştir. Çalışmalarında yazarlar saldırı başarı olasılığını risk matrisi ve normal dağılım kullanarak olasılıksal olarak tanımlamıştır. Bryans vd [16] saldırı-savunma ağaçları kullanarak siber fiziksel sistemlerde (SFS) gerçekleştirilen saldırılar ve savunma yöntemlerinin etkileşimini incelemiştir. Yazarlar SFS modeli, saldırı ve savunma sistemlerinin tanımlandığı şablonlar kullanarak bu ağaçların otomatik olarak çizilmesini sağlayan bir yöntem önermiş ve çizimlerin doğrulamasını yapmıştır.

Saldırı savunma ağaçlarının analizinde kullanılması gereken önemli parametrelerden birisi saldırı başarı olasılığıdır. Siber saldırıların başarı olasılığının hesaplanmasında yaygın zafiyet puanlama sistemi (CVSS) değerlerinin kullanılması kabul edilmiş bir yaklaşımdır [17, 18]. Bu çalışmada, saldırı başarı oranlarının hesaplanmasında CVSS değerleri kullanılacaktır.

Bilişim sistemlerinin risk analizini tanımlarken “Risk = Tehdit x Zafiyet x Sonuçlar” temel yaklaşımı kullanılacaktır. Burada “Tehdit” saldırganın sisteme yapacağı saldırının başarı olasılığını temsil ederken “Zafiyet” ise sistemin dış tehditlere karşı ne denli kırılgan olduğunun bir ölçütüdür. “Sonuçlar” ise başarılı bir saldırının sistemde ortaya çıkaracağı her türlü zararın ekonomik maliyetini temsil etmektedir.

Gelecek bölümlerde, saldırı-savunma ağaçlarının temellerini ve siber risk analizindeki rolü incelenerek gerçekçi hayat örneğine uygulanmıştır. Ayrıca, saldırı-savunma ağaçlarını kullanarak yapılan nicel siber risk analizinin karşılaştığı zorlukları ve dikkate alınması gerekenler tartışılarak bu yaklaşımın çağdaş siber güvenlik paradigmaları ile nasıl uyumlu olduğu incelenmiştir.

II. TEORİK METOT

Bu araştırma, siber risk analizini ilgili parametreler ve saldırı ağacının yapısı dikkate alınarak hesaplama amacını taşımaktadır. Ayrıca, siber riskin en aza indirilmesi için gerekli savunma stratejilerinin ilgili saldırı-savunma ağacı üzerinden belirlenmesi hedeflenmiştir. Genel risk tanımında temel bileşenler olarak tehdit, zafiyet ve olası sonuçlar yer alır ki bu Eş. 1 ile gösterilmiştir. Benzer şekilde, siber güvenlik alanında da risk tanımlaması yapılabilir. Ancak, doğru bir risk hesaplaması için ilgili bileşenlerin siber güvenlik alanına ve dinamiklerine uygun şekilde tanımlanması gerekmektedir. Aksi halde hesaplanan risk ve ilgili risk azaltma önlemleri gerçekçi olmayacaktır.

Bu çalışmada, siber riskin hesaplanabilmesi için saldırı-savunma ağacı kullanılmakta ve bu ağaç üzerinden tüm risk bileşenleri tanımlanarak matematiksel modele eklenmektedir, bu da çalışmamızın özgün yönünü oluşturmaktadır.

Risk = Tehditler x Zaaflar x Sonuçlar (1)

Tablo 1'de mevcut bir siber ağ için saldırı-savunma ağacı kullanılarak riskin hesaplanabilmesi için gerekli indisler, parametreler ve karar değişkenleri verilmiş ve devamında risk denklemleri oluşturularak açıklanmıştır.

Tablo 1. İndisler, Parametreler ve Karar Değişkenleri

İndis	Parametreler ve Karar Değişkenleri
i	Saldırı/saldırı-savunma ağacı üzerindeki her bir tehdit düğümü, $(i \in I)$. Ağaç üzerinde daire şeklinde düğümler ile gösterilmiştir.
$\underset{\sim}{i}$	*i* düğümünün çocuk düğümleri kümesi
d	Saldırı-savunma ağacı üzerinde savunmacı tarafından alınabilecek her bir savunma önlemi, $(d \in D)$. Ağaç üzerinde dikdörtgen şeklinde düğümler ile gösterilmiştir.
T_i	*i* düğümü üzerinde suistimal edilebilir tehdit olma durumu (i düğümü tehditlere açıksa 1, değilse 0 değerini alır).
Z_i	*i* düğümü ile ilişkilendirilebilen zafiyet olma durumu (i düğümü herhangi bir zafiyetle ilişkilendirilmişse 1, değilse 0 değerini alır).
F_i	Saldırganın *i* düğümüne saldırma olasılığı
P_i	*i* düğümü kullanılarak saldırılması durumdaki başarı olasılığı
$CVSS_i$	*i* düğümünü suistimal etmede kullanılabilecek zafiyetlerin normalize edilmiş CVSS değerlerinin en büyüğü (*i* düğümü herhangi bir zafiyete sahip değilse 0 değerini alır).
S	Yapılan saldırının başarılı olması durumunda savunucuya vereceği zararın sayısal değeri
Q_{id}	Savunmacının d önlemini alması durumunda *i* düğümü üzerinde saldırganı caydırabilme (deterrence) oranı. (*i* düğümü üzerinde alınamayacak önlemler için 0 değerini alır).
L_{id}	Savunmacının d önlemini alması durumunda *i* düğümünün siber saldırılar karşısında zafiyet skorunu azaltma (mitigation) seviyesi (*i* düğümü üzerinde alınamayacak önlemler için 0 değerini alır).
K_{id}	Tehdit düğümü (*i*) savunma yöntemi (*d*) ilişki matrisi
M_{id}	Savunmacının *i* düğümü üzerinde d önlemini almasının maliyeti
B	Toplam savunma bütçesi
R_i^y	*i* bir yaprak düğüm ise siber risk seviyesi
R_i^d	*i* düğümü üzerinde önlem(ler) alınması durumunda risk seviyesi
R_i^{OR}	*i* bir yaprak düğüm değil ise ve OR (veya) ilişkili çocuk düğümlere sahip ise siber risk seviyesi
R_i^{AND}	*i* bir yaprak düğüm değil ise ve AND (ve) ilişkili çocuk düğümlere sahip ise siber risk seviyesi
x_{id}	Savunmacı *i* düğümü üzerinde d önlemini alırsa 1, aksi takdirde 0 olan ikili karar değişkeni

Risk Fonksiyonları

$$R_i^y = (T_i * F_i * P_i) * (Z_i * CVSS_i) \quad (2)$$

$$R_i^d = \left\{T_i * F_i * (1 - \underset{d \in D}{\text{enb}}(K_{id} Q_{id} x_{id})) * P_i\right\} * \left\{Z_i * (CVSS_i - \underset{d \in D}{\text{enb}}(K_{id} L_{id} x_{id}))\right\} \quad (3)$$

$$R_i^{OR} = 1 - \prod_{i \in \underset{\smile}{i}} (1 - R_i) \quad (4)$$

$$R_i^{AND} = \underset{i \in \underset{\smile}{i}}{\text{enk}}(R_i) \quad (5)$$

$$\sum_i \sum_d M_{id} x_{id} \leq B \quad (6)$$

Burada Eş. 2 mevcut sistemin risk seviyesini ölçmektedir. Risk bileşenlerinden ilki olan tehdit üç parametre değerinin çarpımıyla elde edilir. Buna göre saldırı ağacı üzerindeki herhangi bir *i* yaprak düğümü tehditlere yapısı gereği açıksa ($T_i = 1$) saldırganın bu düğüm üzerinden sisteme saldırma olasılığı geçmiş veriler üzerinden hesaplanır ve eğer bir saldırı gerçekleşirse bu saldırının başarılı olma olasılığı ile çarpılarak ilgili düğüm üzerindeki tehdit seviyesi ölçülmüş olur. Risk ölçümünün diğer bir bileşeni olan zafiyet ise ilgili düğümün zafiyeti varsa ($Z_i = 1$) bunun ilgili CVSS skoru ile çarpılması ile ölçülür.

Gerekli savunma önlemleri Eş. 6'da verilen bütçe kısıtına göre alınması durumunda risk seviyesi Eş. 3 kullanılarak hesaplanabilir. Burada Eş. 2'ye benzer şekilde her bir yaprak düğüm için tehdit ve zafiyet seviyeleri çarpılarak risk ölçülür. Ancak, savunmacı tarafından i yaprak düğümü üzerinde uygulanan önlem sayesinde saldırganı caydırma seviyesi saldırı olasılığını azaltacağı için denkleme $F_i * (1 - \underset{d \in D}{\text{enb}}(K_{id} Q_{id} x_{id}))$ şeklinde eklenmiştir. Benzer şekilde, savunmacının alacağı önlemler ilgili düğümdeki zafiyet seviyesini düşüreceği için bu durum CVSS skorunun azalması şeklinde $CVSS_i - \underset{d \in D}{\text{enb}}(K_{id} L_{id} x_{id}))$ denkleme yansıtılmıştır. Burada, aynı düğüm üzerinde birden fazla önlem alındığında bunların caydırıcılık ve zafiyeti azaltma konusunda etkisi genellikle en etkili olanla ölçüldüğü varsayılmıştır. Sonuç olarak, kısıtlı bütçe altında riski en küçükleyecek savunma stratejileri Eş. 3 ve 6 kullanılarak hesaplanır.

Yaprak düğümlerin risk seviyeleri ölçüldükten sonra ara düğümlerin ve nihayet kök düğümün risk seviyesini ölçebilmek için saldırı ağacında yapraklardan düğümlere doğru risk değerleri Eş. 4 ve 5 kullanılarak aktarılır. Eğer, ebeveyn düğümün çocuk düğümleri "OR" (veya) kombinasyonuna sahipse Eş. 4, "AND" (ve) kombinasyonuna sahipse de Eş. 5 kullanılarak risk değerlemesi yapılır. Bu iteratif yaklaşım kök düğümün risk seviyesi hesaplanıncaya kadar sürdürülür. Son olarak, hesaplana kök düğüm risk seviyesi saldırının potansiyel maliyet değeri ile çarpılarak (*S*) ilgili sistemin siber riski hesaplanmış olur.

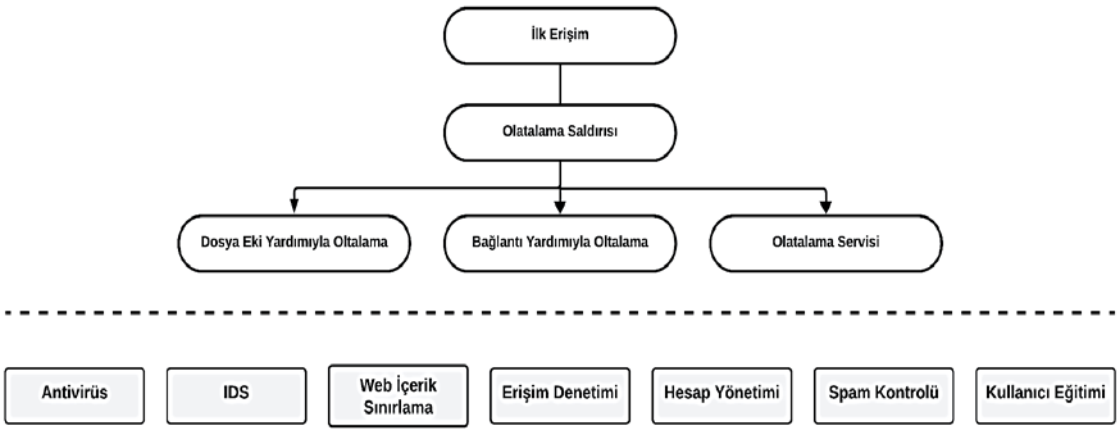
III. BULGULAR VE TARTIŞMA

Bu çalışmada önerilen risk hesaplama ve analiz yaklaşımı oltalama saldırılarının oluşturduğu riski hesaplayacak bir örnek uygulama ile bu bölümde sunulacaktır. Oltalama saldırıları internet kullanıcılarının hassas bilgilerini kişilerin güvendiği şahıs veya kurum kimliklerini kullanarak yasal olmayan yollar ile elde etmeyi hedefleyen sosyal mühendislik saldırılarıdır [19]. Proofpoint'in yayınladığı rapora göre 2019 yılında işletmelerin %90'ı oltalama saldırılarına maruz kalmıştır [20]. Bu saldırıların işletmeler üzerinde oluşturduğu risk ihmal

edilemeyecek kadar büyüktür. Bu örnek olay incelemesinde saldırı- savunma ağacı kullanarak oltalama saldırısının sebep olduğu riski hesaplanacak ve analiz edilecektir.

MITRE ATT&CK [21] tarafından yayınlanan işletmeler için taktikler ve teknikler tablosunda oltalama saldırıları ilk erişim taktikleri altında bir teknik olarak listelenmiştir. Bu çalışmada kullanılan saldırı- savunma ağacı da MITRE ATT&CK sınıflandırması temel alınarak oluşturulmuştur.

Şekil 3'te MITRE ATT&CK tarafından tanımlanmış oltalama saldırıları sınıflandırması ve bu saldırılara karşı kullanılan savunma yaklaşımları gösterilmiştir. Şekil 3'teki sınıflandırma ve ilişkilerden faydalanılarak çizilen oltalama saldırısına ait saldırı-savunma ağacı Şekil 4'te gösterilmektedir. Bu örnek çalışmada sistem erişimi tehdidine karşı oltalama saldırılarının oluşturduğu risk hesaplanacaktır. Bu sebeple çizilen saldırı-savunma ağacının kök düğümü olarak oltalama saldırısının hedefi olan sistem erişimi yazılmıştır. Ağacın takip eden seviyesine saldırı hedefine ulaşabilmek için birlikte olması gereken zararlı yazılımın dağıtımı ve bu yazılımın çalıştırılmasını temsil eden çocuk düğümler eklenmiştir. Zararlı yazılımın elektronik posta üzerinden dağıtımı yapılabileceğini gösteren düğüm dağıtım kök düğümü altına eklenmiştir. Ayrıca elektronik posta ile dağıtım esnasında kullanılabilecek dosya eklentisi veya bağlantı adresi de birer çocuk düğüm olarak ağaca eklenmiştir.



Şekil 3. MITRE ATT&CK oltalama saldırısı sınıflandırması ve savunma yöntemleri

Oltalama saldırısının başarılı olarak gerçekleşmesi için dağıtım işleminin tamamlanması sonrası zararlı yazılımın çalıştırılması gerekmektedir. Ağaçta çalıştırma düğümünün altına işlemin kullanıcı tarafından manuel olarak yapılabileceğini gösteren çocuk düğüm de eklenmiştir.

Oluşturulan saldırı ağacına ilgili tehditlere karşı kullanılabilecek savunma mekanizmaları uygun seviyelerde eklenerek saldırı- savunma ağacı oluşturulmuştur. Ağacın çizimi sonrası analiz ve hesaplama sürecinde ihtiyaç duyulacak saldırı ve savunma başarı olasılıkları tanımlanmıştır. Risk hesaplamasında kullanılacak tehdit bileşenlerinden tehdit vektörü çizilen saldırı- savunma ağacında suistimal edilebilir tehditler belirlenerek, ilgili tehditlere karşı saldırı olasılıkları hedef kurumun bilgi işlem istatistiklerinden ve saldırı başarı olasılıkları dönemlik siber güvenlik raporları incelenerek çıkarılabilir. Riskin zafiyet bileşenlerinden zafiyet vektörü ilgili tehdidi aktif kılan güvenlik açığı olarak tanımlanıp bilişim sistemi zafiyet taraması sonucu bulunabilir ve etkisi CVSS değerleri

kullanılarak hesaplanabilir. Riskin sonuç bileşeni ise saldırının başarılı olması halinde hedef kuruma maliyeti olarak tanımlanıp, kurum özelinde kullanıcı tarafından girilebilir.

Saldırı ağaçları ile risk hesaplaması sürecinde tehditlere, zafiyetlere ve sonuçlara odaklanılıp savunma mekanizmalarının etkisi genellikle sürece direkt dahil edilmemektedir. Bu çalışmada kullanılan saldırı- savunma ağacı yardımı ile savunma mekanizmaları ağaca eklenebilmiş ve risk hesaplaması sürecine savunma bileşenleri hesaba katılmıştır. Bu bileşenlerden savunma vektörü tehditlere karşı kullanılabilecek savunma mekanizmalarını, savunucu başarısızlık oranı kullanılan savunma yaklaşımının ilgili tehdide karşı sistemi koruyamama olasılığını ve savunucu karar vektörü kurumun olası savunma yöntemlerinden hangilerini kullanıldığını belirtir. Hesaplama sürecinde ihtiyaç duyulacak savunma vektörü MITRE ATT&CK veri tabanından, savunucu başarısızlık oranı kullanılan savunma ürünlerinin teknik dokümantasyonu veya yayınlanan performans göstergelerinden ve savunucu karar vektörü kurum bilgi işlem biriminden temin edilebilir.

Şekil 4'te görülen saldırı-savunma ağacında tehdit ve savunma düğümleri *i* ve *d* olarak işaretlenmiş ve numaralandırılmıştır. Suistimal edilebilir tehditler ağacın yapraklarında gösterilmiş olup bu yaprakların ata düğümleri saldırının ağaç üzerindeki mantıksal rotasını göstermekte olup risk hesaplamasında etkisi yoktur. Verizon tarafından yapılan bir analize göre başarılı olarak gerçekleşen saldırıların %90'ı oltalama saldırısı içermektedir [22]. Proofpint'in 2019 da yayınladığı rapora göre oltalama saldırılarının %10'u e-posta eki ile gerçekleşirken %90'ında zararlı bağlantılar kullanılmaktadır. Bu bilgiler ışığında I_5 ve I_6 düğümleri üzerinden saldırı olasılıkları için sırasıyla $F_5 = 0.1$ ve $F_6 = 0.9$ değerleri kullanılmıştır. Graphus tarafından yayınlanan rapora göre gerçekleştirilen oltalama saldırılarının %65'i başarılı olmaktadır [23]. Bu çalışmada oltalama saldırısına katkı sağlayan tehdit düğümleri kullanılarak suistimal gerçekleştirme (exploit) olasılığı P_i değerleri 0.65 kabul edilmiştir. Almanya Friedrich-Alexander Üniversitesinde yapılan bir çalışmaya göre risklerden haberdar olmalarına rağmen kullanıcıların %56'sının oltalama saldırısı dosyalarını çalıştırdığı veya bağlantıları açtığı gözlemlenmiştir [23]. Bağlı olarak I_4 düğümü için F_4 değeri 0,56 olarak kullanılmıştır.

Zafiyet taraması sonucu elde edilecek zafiyetler ile ilişkilendirilebilecek tehdit düğümleri zafiyet vektörü Z'de 1 olarak işaretlenmiştir. Her bir tehdit düğümü ile ilişkili zafiyetlerden etkisi en yüksek olan CVSS değeri CVSS vektörüne yazılmıştır. Bu çalışmada oltalama saldırılarında sıklıkla suistimal edilen CVE-2017-11882 uzaktan kod çalıştırma ve CVE-2023-35120 siteler arası çağrı sahteciliği (cross-site request forgery) zafiyetlerinin var olduğu varsayılmıştır. Bu zafiyetlerin ilişkili olduğu tehdit düğümleri Tablo 2'de gösterilmiştir.

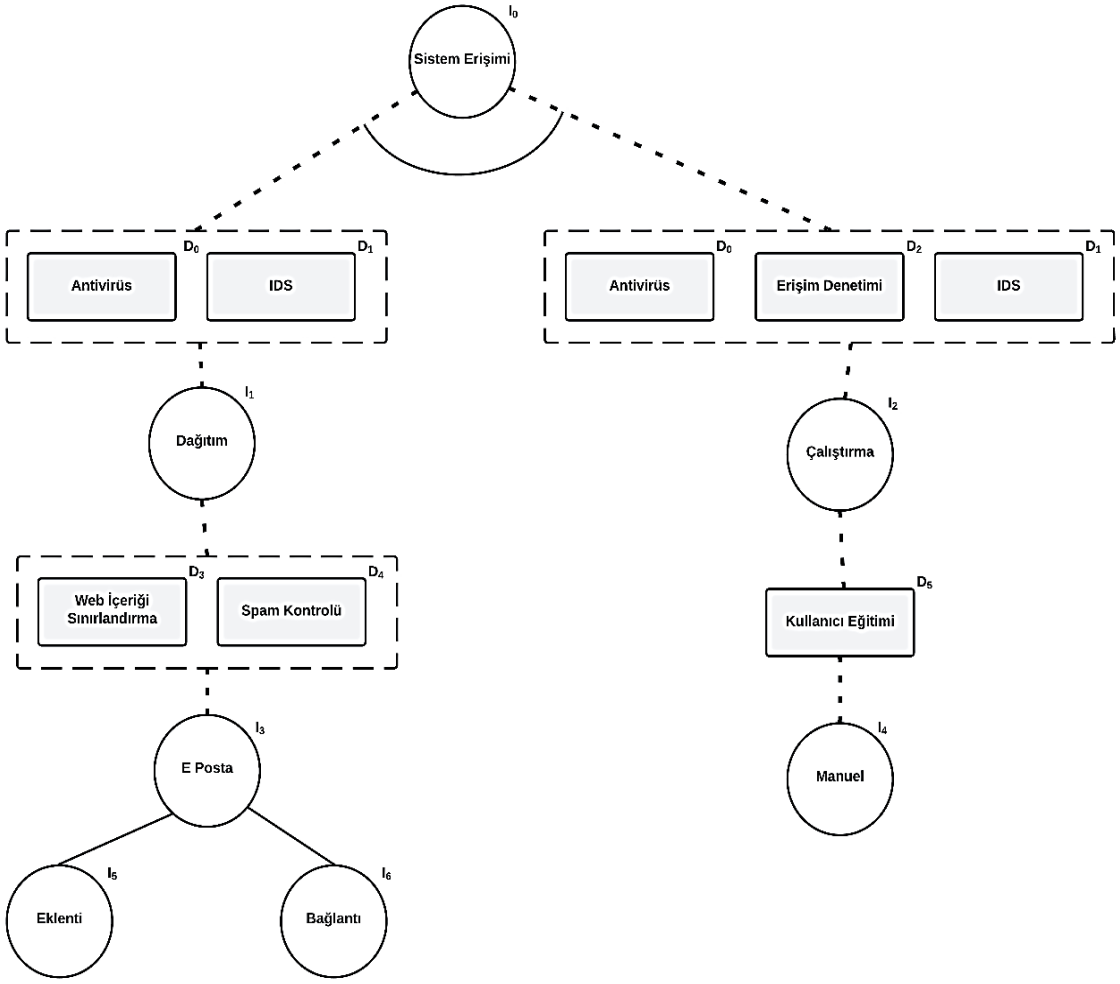
Tablo 2. Zafiyet tehdit düğüm ilişkisi matrisi ve zafiyetlerin CVSS skorları

Zafiyet	**I_4**	**I_5**	**I_6**	**CVSS Skoru**
CVE-2017-11882	1	1	0	7.8
CVE-2023-35120	0	0	1	8.8

Ağaç üzerinde farklı tehditlere karşı kullanılabilecek farklı savunma yöntemleri bir bütün olarak sunulmuştur. Savunmacı bu savunma yöntemlerinden bütçesine bağlı olarak uygun olanları sistemine ekleyecektir. Tablo 3'te ağaçta bulunan tehditler ve bu tehditlere karşı kullanılabilecek savunma yöntemlerinin ilişkilendirilmesi yapılmıştır. Tablo 3'te bir ile gösterilen hücreler bir savunma yönteminin ilgili tehdide karşı kullanılabileceğini ifade ederken, 0 ile savunma yönteminin ilgili tehdide karşı bir etki sağlamadığı gösterilmiştir.

Tablo 3. Tehdit-savunma yöntemi ilişki matrisi (K_{id}) ve Q_{id} değerleri

Savunma Yöntemi	**I_4**	**I_5**	**I_6**	**Q_{id}**
Antivirüs (D_0)	1	1	1	0,90
IDS (D_1)	1	1	1	0,97
Erişim Denetimi (D_2)	1	0	0	0,97
Web İçerik Sınırlama(D_3)	0	1	1	0,98
Spam Kontrolü (D_4)	0	1	1	0,872
Kullanıcı Eğitimi (D_5)	1	0	1	0,79



Şekil 4: Oltalama saldırısı saldırı-savunma ağacı

Savunma amaçlı kullanılan yöntemlerin başarısı tehdit ve zafiyet seviyelerini etkileyecektir. Bu çalışmada kullanılan savunma yöntemlerinin başarı seviyeleri, güvenlik raporları, çevrimiçi ürün performans sıralamaları ve akademik çalışma sonuçlarına göre seçilmiştir. AntivirusGuide web sitesinde yayınlanan antivirüs yazılımlarına oltalama saldırılarına karşı verilen başarı değerlendirmesi [24] referans alınarak D_0 değeri %90 kabul edilmiştir. Shah ve Issac'ın [25] gerçekleştirdiği IDS performans kıyaslaması çalışmasında IDS başarısı %97 olarak ölçülmüş olup D_1 savunma düğüm başarısı 0,97 kabul edilmiştir. Qiang vd. [26] sistem kontrol akışlarını takip ederek %97 başarımla zararlı yazılımları tespit etmiştir ve D_3 değeri buna bağlı olarak 0,97 kabul edilmiştir. Microsoft Araştırma grubu tarafından zararlı web bağlantı tespit çalışmasında Choi vd. [27] %98 başarı elde etmiştir ve bağlı

olarak D_5 değeri 0,98 seçilmiştir. Kaspersky Araştırma grubundan Tushkanov'un raporuna [28] göre ChatGPT gibi büyük dil modelleri kullanarak yapılan spam engelleme çalışmalarında %87,2 başarı elde edilmiş olup D_6 değeri 0,872 seçilmiştir. Verizon tarafından 2016 yılında yapılan çalışma sonuçlarına göre [23] oltalama saldırı başarısı farkındalık eğitimi sonrası %79 azalmıştır. Bu bilgi ışığında da D_7 değeri 0,79 seçilmiştir.

Yapılan örnek olay çalışmasında savunma yaklaşımlarının risk üzerindeki etkisini göstermek için önce savunmasız sistem riski (S_0) hesaplanmıştır. Takip eden senaryolarda farklı savunma karar vektörleri (x_{id}) kullanılarak risk değerleri hesaplanmıştır. Bu senaryolar sırasıyla tüm teknik imkanları kullanarak savunma S_1, teknik savunmaya ilave kullanıcı eğitimi S_2 ve bireysel kullanıcı için temel risk senaryosu S_3 listelenmiş ve Tablo 4'te gösterilmiştir. Bu senaryolarda kullanılan savunma yöntemlerine bağlı CVSS değişimleri Tablo 5'te gösterilmiştir. Bu değerler ilgili zafiyetin CVSS hesap makinesinde baz değerlendirme metriklerinden etki metrikleri değiştirilerek elde edilmiştir. Elde edilen bu sonuçlar tartışma bölümünde detaylı olarak değerlendirilmiştir.

Tablo 4. Çeşitli savunma senaryoları için hesaplanan siber risk seviyeleri (S_0: Savunmasız durum, S_1: Yalnız teknik savunma durumu, S_2: Kullanıcı eğitimi ile desteklenmiş teknik savunma durumu, S_3: Bireysel kullanıcılar için temel savunma durumu)

Savunma Senaryosu	D_1	D_2	D_3	D_4	D_5	D_6	Risk Seviyesi
S_0	-	-	-	-	-	-	0,28392
S_1	✓	✓	✓	✓	✓	-	0,00721
S_2	✓	✓	✓	✓	✓	✓	0,00579
S_3	✓	-	-	-	✓	-	0,02657

Tablo 5. Farklı savunma senaryolarına bağlı CVSS değer değişim tablosu

Savunma Senaryosu	$CVSS_4$	$CVSS_5$	$CVSS_6$
S_0	7.8	7.8	8.8
S_1	6.6	6.6	7.6
S_2	5.3	5.3	6.3
S_3	7.3	7.3	8.3

IV. SONUÇLAR

Bu çalışma kapsamında saldırı-savunma ağacı kullanılarak siber risk hesaplamasında kullanılabilecek gerçekçi bir model sunulmuştur. Sunulan modele ait tüm parametrelerin hangi kaynaklardan temin edilebileceği belirtilmiş ve önerilen bu yöntem oltalama saldırılarına karşı risk hesaplaması örnek olay incelemesinde kullanılmıştır.

Çalışma kapsamında yapılan örnek olay incelemesinde kullanılan saldırı-savunma ağacı MITRE ATT&CK referans alınarak oluşturulmuştur. Bu çalışmada gerçekçi sonuçlar elde edebilmek için hesaplamalarda kullanılan parametre değerleri siber güvenlik raporları, ürün değerlendirme çalışmaları ve akademik yayınlardan alınmıştır.

Geliştirilen risk modeli kullanılarak önce oltalama saldırılarına karşı savunmasız bir sistem risk değeri (0,28392) hesaplanmıştır. Daha sonra sırasıyla bu saldırılara karşı kullanılabilecek yöntemleri kullanan teknik savunma senaryosu ve ilave olarak kullanıcı farkındalık eğitiminin etkisini gösteren senaryolarda risk hesaplaması yapılmıştır. Son olarak bir ev kullanıcısının sahip olduğu temel savunma bileşenlerine bağlı risk hesaplaması yapılmıştır. Elde edilen risk değerlerinin sistem girdileri ile tutarlı olduğu gözlemlenmiştir. Literatür ve internette yaptığımız aramalar, siber risk hesaplamasında standart bir yöntemin olmadığını göstermiştir. Önerdiğimiz risk hesaplama modelinin alanda öncü olacağını öngörmekteyiz.

Ek olarak geliştirdiğimiz bu model bilişim sistemlerin bileşenlerinin sistemin başarılı bir şekilde çalışması için önemleri veya bir saldırıya karşı savunmasızlık düzeyleri açısından ve tehditlerin oluşturduğu tehlike ve olasılıkları açısından önceliklendirilmesine yardımcı olacaktır. Ayrıca, bilişim sistemlerinin yöneticilerine ve mühendislerine, yeterli güvenlik politikalarının geliştirilmesinde, güvenli sistemlerin tasarımında ve genellikle kıt kaynakların rasyonel dağılımında yardımcı olacaktır. Ayrıca güvenlik, iş ve bilişim uzmanları arasındaki iletişimi de kolaylaştıracaktır ve sigorta şirketleri tarafından siber risk sigorta primlerinin hesaplanmasında kullanılabilecektir.

KAYNAKLAR

[1] Strupczewski G (2021) Defining cyber risk. Safety science, 135, 105143.
[2] Aldasoro I, Gambacorta L, Giudici P, Leach T (2022) The drivers of cyber risk. Journal of Financial Stability, 60, 100989.
[3] Jamilov R, Rey H, Tahoun A (2021) The anatomy of cyber risk (No. w28906). National Bureau of Economic Research.
[4] Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, Materne S (2022) Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on risk and insurance-Issues and practice, 47(3), 698-736.
[5] Eling M, McShane M, Nguyen T (2021) Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125.
[6] Sheyner O, Haines J, Jha S, Lippmann R, Wing JM (2002) Automated generation and analysis of attack graphs. In Proceedings 2002 IEEE Symposium on Security and Privacy (pp. 273-284). IEEE.
[7] Nagaraju V, Fiondella L, Wandji T (2017) A survey of fault and attack tree modeling and analysis for cyber risk management. In 2017 IEEE International Symposium on Technologies for Homeland Security (HST) (pp. 1-6). IEEE.
[8] Haque MA, Haque S, Kumar K, Singh NK (2021) A comprehensive study of cyber security attacks, classification, and countermeasures in the internet of things. In Handbook of research on digital transformation and challenges to data security and privacy (pp. 63-90). IGI Global, Pennsylvania, USA.
[9] Kordy B, Mauw S, Radomirović S, Schweitzer P (2014) Attack–defense trees. Journal of Logic and Computation, 24(1), 55-87.
[10] Bagnato A, Bíró RK, Bonino D, vd. (2017) Designing swarms of cyber-physical systems: The H2020 CPSwarm project. In Proceedings of the Computing Frontiers Conference (pp. 305-312).
[11] He S, Lei D, Shuang W, Liu C, Gu, Z (2020) Network Security Analysis of Industrial Control System Based on Attack-Defense Tree. In 2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS) (pp. 651-655). IEEE.
[12] Rios E, Rego A, Iturbe E, Higuero M, Larrucea X (2020) Continuous quantitative risk management in smart grids using attack defense trees. Sensors, 20(16), 4404.
[13] Guo H, Ding L, Xu W (2022) Cybersecurity Risk Assessment of Industrial Control Systems Based on Order-α Divergence Measures Under an Interval-Valued Intuitionistic Fuzzy Environment. IEEE Access, 10, 43751-43765.
[14] Hyder B, Majerus H, Sellars H, vd. (2022) CySec Game: A Framework and Tool for Cyber Risk Assessment and Security Investment Optimization in Critical Infrastructures. In 2022 Resilience Week (RWS) (pp. 1-6). IEEE.
[15] Mondal SK, Tan T, Khanam S, Kumar K, Kabir HMD, Ni K (2023) Security Quantification of Container-Technology-Driven E-Government Systems. Electronics, 12(5), 1238.
[16] Bryans J, Liew LS, Nguyen HN, Sabaliauskaite G, Shaikh SA (2023) Formal Template-Based Generation of Attack–Defence Trees for Automated Security Analysis. Information, 14(9), 481.
[17] Houmb SH, Franqueira VN, Engum EA (2010) Quantifying security risk level from CVSS estimates of frequency and impact. Journal of Systems and Software, 83(9), 1622-1634.
[18] Wu W, Kang R, Li Z (2015) Risk assessment method for cyber security of cyber physical systems. In 2015 First International Conference On Reliability Systems Engineering (ICRSE) (pp. 1-5). IEEE.
[19] Jakobsson M, Myers S (Eds.) (2006) Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, New York, USA.
[20] Proofpoint (2020) State of the Phish An in-depth look at user awareness, vulnerability and resilience. Web. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf Erişim: 23 Ekim 2023.
[21] MITRE Corporation (2023) MITRE ATT&CK. Web.https://attack.mitre.org/ Erişim: 23 Ekim 2023.

[22] GARPHUS Kaseya Company (2020) Verizon Says Phishing Still Drives 90% of Cybersecurity Breaches. Web. https://www.graphus.ai/blog/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/ Erişim: 23 Ekim 2023.
[23] GARPHUS Kaseya Company (2023) Spear Phishing & Social Engineering. People are your weakest cybersecurity link. What are you going to do about it? Web. https://www.graphus.ai/resources/spear-phishing-social-engineering/ Erişim: 23 Ekim 2023.
[24] AntivirusGuide (2023) The Best Anti-Phishing Software Of 2023 Web. https://bit.ly/TheBestAnti-PhishingSoftwareOf2023 Erişim: 23 Ekim 2023.
[25] Shah, SAR, Issac B (2018) Performance comparison of intrusion detection systems and application of machine learning to Snort system. Future Generation Computer Systems, 80, 157-170.
[26] Qiang W, Yang L, Jin H (2022) Efficient and robust malware detection based on control flow traces using deep neural networks. Computers & Security, 102871.
[27] Choi H, Zhu BB, Lee H (2011) Detecting malicious web links and identifying their attack types. In 2nd USENIX Conference on Web Application Development (WebApps 11).
[28] Vladislav Tushkanov (2023) What does ChatGPT know about phishing? Web. https://securelist.com/chatgpt-anti-phishing/109590/ Erişim: 23 Ekim 2023.