ÇOK NİTELİKLİ FAYDA TEORİSİYLE SALDIRGAN PROFİLİNE YENİ PARAMETRELERİN EKLENMESİ

Erdal IRMAK[1], İsmail ERKEK[2]
[1]Gazi Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü, Ankara, Türkiye
[2]Gazi Üniversitesi Bilgi Güvenliği Mühendisliği ABD, Ankara, Türkiye
erdal@gazi.edu.tr, ismailerkek2014@gmail.com

ÖZET

Bilgi güvenliği alanında risk değerlendirmesi siber saldırılara karşı alınacak önlemlerin en başlarında yer almaktadır. Bunun gerçekleştirilebilmesi için tehdit türlerinin çok iyi analiz edilmesi gerekmektedir. Bu çalışmada, kritik bilgi sistemlerine yönelik siber saldırı gerçekleştiren saldırganların profilleri incelenmiş, saldırı ağacı modeliyle saldırı başarı ihtimallerinin hesaplanması ve analizi yapılmıştır. Literatürde yer alan saldırgan profili parametrelerinde bir takım karakteristik özelliklerinin eksikliği fark edilmiş ve eksikliği fark edilen bu karakteristik özellikler saldırgan profiline eklenerek matematiksel olarak saldırı başarı ihtimali gerçeğe daha yakın olarak ifade edilmiştir.

Anahtar Kelimeler: Risk değerlendirmesi, Saldırgan Profili, Saldırı Ağacı, Bilgi Güvenliği

ADDING NEW PARAMETERS TO ATTACKER PROFILE BY USING MULTI-ATTRIBUTE UTILITY THEORY

ABSTRACT

Risk assessment takes place in the head of the measures to be taken against cyber attacks in the field of information security. Threat types should be analysed resplendently to carry out this issue. In this study, profiles of attackers who performed cyber attacks on critical information systems have been researched, calculating and analysing the probabilities of success of attack with attack tree model have been performed. The absence of a number of characteristics in the attacker profile parameters located in the literature has been noticed. Probability of success attacks has been expressed closer to the truth mathematically by adding characteristics that is awared of absence to the attacker profile.

Keywords: Risk Assessment, Attacker Profile, Attack Tree, Information Security

1. GİRİŞ (INTRODUCTION)

Bilgi ve iletişim teknolojilerinin gelişmesine paralel olarak bu sistemlerin güvenlik açıklarında da ciddi artışlar olduğu gözlenmektedir. Siber saldırıları gerçekleştiren saldırganlar bu güvenlik açıklarını istismar ederek kritik bilgi sistemlerine zarar verebilmekte, erişilemez kılmakta, gizliliğini ifşa etmekte ve verilerin bütünlüğünü bozabilmektedir. Bu sebeple bilgi güvenliğinin ilk adımlarından olan risk değerlendirmesinin en iyi şekilde uygulanması gerekmektedir. Varlıklar için risk temel olarak "Oluştuğu zaman, varlığın değerini azaltan bir olayın olasılığı" şeklinde tanımlanabilir [1]. Bilgi güvenliği açısından ise bilgi varlığının maddi ve manevi olarak değerini azaltan ve bilgi varlığındaki bir açıklığın bir tehdit tarafından kullanılma olasılığı olarak tanımlanabilir. Buradan da anlaşılacağı gibi risk hesaplamasında varlık, açıklık ve tehdit olmak üzere bilgi varlığının 3 adet girdisi bulunmaktadır [2].

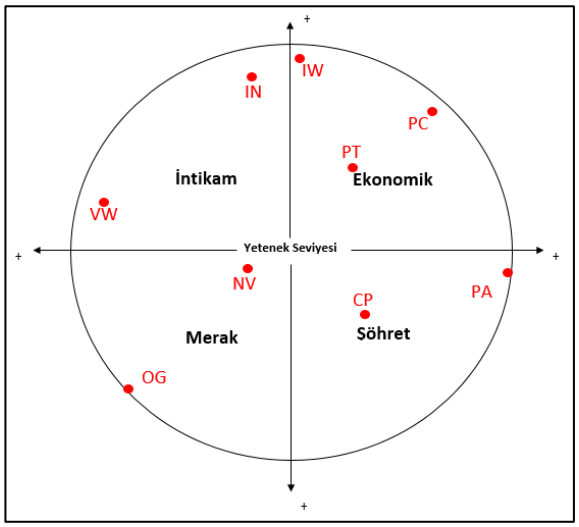
$$Risk = f(varlık, açıklık, tehdit) \quad (1)$$

Bu değişkenlerden tehdit parametresi; insani/insani olmayan faktörler, ağ/fiziksel, teknik/çevresel, içerden/dışarıdan ve kasıtlı/kazara kaynaklı tehditler olarak sınıflandırılabilir [3]. Kurum ve kuruluşlardaki bilgi güvenliğine yönelik tehditlerin çoğu insani faktörlerden kaynaklanmaktadır. İnsani faktörler de kendi içerisinde dış ve iç kaynaklı olarak iki şekilde sınıflandırılabilir. Dış kaynaklı faktörler; virüs, DDoS,

web sayfası değişimi saldırısı şeklinde, iç kaynaklı olaylar; kurumdaki mevcut ve eski çalışanların e-mail okuması, yetkisiz bilgilere erişimi, önceki hakların kullanımı ve gizli bilgilerin ifşası şeklinde gerçekleşmektedir.

Saldırgan profillerinin türleri, gelişimi, sınıflandırılması ve analizi; saldırgan profili parametrelerinin belirlenmesi ve matematiksel olarak ifade edilmesi için çok önemlidir. Tehdit türlerinin insani faktörleri arasında yapılan literatür araştırmasında saldırganların farklı motivasyon çeşitlerine göre sınıflandırıldığı ve analiz edildiği gözlenmiştir. Rogers'ın yaptığı çalışmada [4] saldırganların gelişiminde 2 boyutlu çember modeli kullanılarak saldırganların birçok türü tanımlanmıştır. Saldırganların teknik, kabiliyet ve motivasyon açısından 8 farklı profili çıkarılmıştır. Saldırganların motivasyonuna göre; intikam, ekonomik, merak ve şöhret olmak üzere 4 farklı tür belirlenmiştir. Şekil 1'de merkezden uzağa gidildikçe saldırganın teknik kabiliyeti artmakta ve dairenin her bir çemberi bir motivasyon kategorisini göstermektedir. Şekilde yer alan saldırgan tanımlamaları aşağıdaki gibi ifade edilebilir:

- Acemi: NV (Novice)
- Siber-acemi: CP (Cyber-punks)
- Kurum içi Çalışan: IN (Internal)
- Acemi Hırsız: PT (Petty Thieves)
- Virüs Yazılımcısı: VW (Virus Writers)
- Eski Kafalı Hacker: OG (Old Guard Hacker)
- Profesyonel Suçlu: PC (Professional Criminals)
- Bilgi Savaşçıları: IW (Information Warriors)



Şekil 1. Saldırganların gelişiminde 2 boyutlu çember modeli (2-Dimensional Circle Model in Hackers Taxonomy)

ICS-CERT'in raporuna göre ise [5]; saldırgan profilleri; teknik yeterlilik ve motivasyon parametreleri baz alınarak aşağıdaki gibi sınıflandırılmıştır.

Yabancı Devletler: Bu kategorideki profillerin yaratacağı tehdit, propagandadan web sayfalarının değişmesine, casusluktan ciddi fiziksel zararlar verecek etkilere sebep olabilir. Bu profildeki saldırganlar özellikle kritik altyapılara ve bilgi sistemlerine uzun süreli zarar verebilir ve geniş alana yayılabilecek etkilere sebep olabilecek saldırılar gerçekleştirebilir. Hedef aldığı ülkenin ulusal güvenliğini tehlikeye sokar.

Teröristler: "Bombalar hala baytlardan daha etkilidir" anlayışından dolayı bu profildeki saldırganlar hedef aldığı ülkenin bilgi sistemlerine zarar vermeye odaklı olup sınırlı bir siber tehdittir. Toplumda endişeyi ve kargaşayı artıracak saldırıları planlarlar.

Casuslar ve organize suç örgütleri: Uluslararası casuslar ve organize suç örgütleri bu kategoride yer almakta olup endüstriyel casusluk ve yüksek miktarda kanun dışı maddi kazanç sağlamayı hedeflemektedirler.

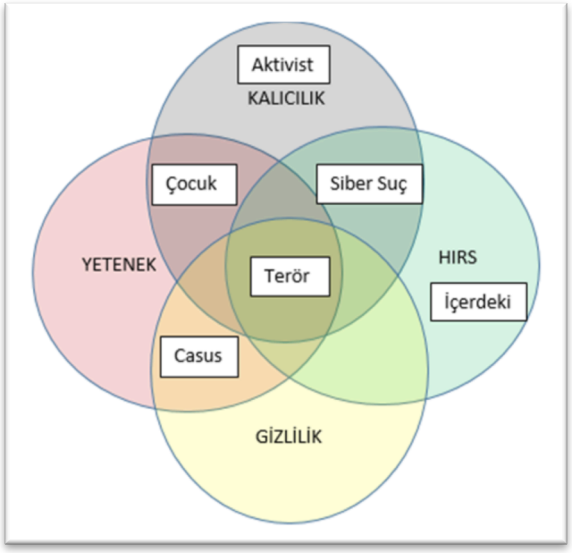
Hacktivistler: Ülkedeki düzene karşı çıkan, politik motivasyonlu, grup halinde veya kişisel çalışan saldırgan profilidir. Orta seviyeli bir tehdit olarak düşünülür fakat sistemlere ciddi zararları olabilir. Bilinen uluslararası hacktivist grupları kritik altyapılara zarar vermek yerine siyasi düşüncelerini yansıtmak için propaganda yaparlar.

Saldırganlar (Hackers): Siber dünyada gerçekleşen saldırıların birçoğu, bu işi hobi olarak yapan kişiler tarafından gerçekleşmektedir. Bu profilde yer alan saldırganların birçoğu kendini siber dünyada ispatlamak, maddi kazanç sağlamak, kritik altyapılara ve bilgi sistemlerine zarar vermek gibi motivasyonlara sahiptir. Saldırgan profillerindeki en geniş kitleyi bu grup oluşturur.

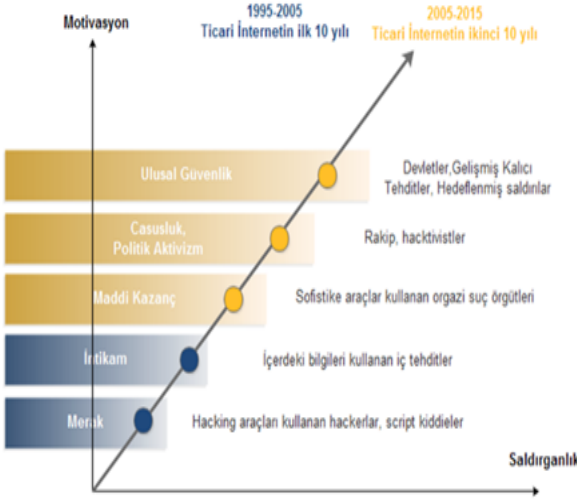
SANS Enstitüsü'nde, siber saldırganların psikolojik ve davranışsal analizlerini yaptığı çalışmada [6], saldırganları tehdit türlerine göre Şekil 2'deki gibi sınıflandırmıştır.

Şekil 3'te ise internetin gelişmesiyle birlikte saldırganların amacındaki değişim ve zaman içerisindeki karmaşıklığı, saldırganlık türleri üzerinde hacker motivesi baz alınarak gösterilmiştir [7].

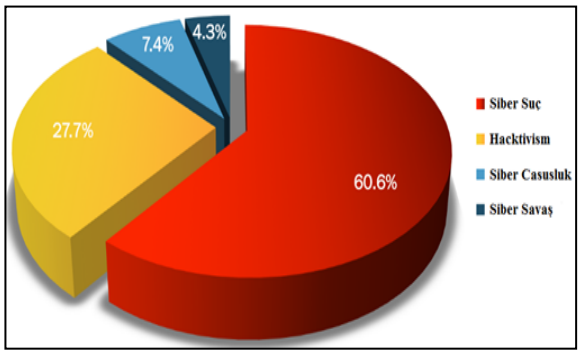
Farklı motivasyonlara sahip 2016 yılında gerçekleşen siber saldırılara ait istatistikler Şekil 4'te gösterildiği gibidir. Gerçekleşen saldırıların istatistiğine göre; saldırganların maddi kazanç sağlamak ve politik düşüncelerini göstermek amacıyla bilgi sistemlerine saldırma olasılığı daha yüksektir. Öte yandan siber casusluk ve siber savaş amacıyla gerçekleşen saldırıların bilgi sistemleri üzerinde oluşturacağı risk daha yüksektir, çünkü bu tehditleri gerçekleştiren saldırganlar ya devletler tarafından desteklenmekte ya da direk olarak devletler tarafından gerçekleştirilmektedir. Ayrıca hedef alınan sistemler ulusal güvenliği ilgilendiren sistemler olduğundan etkisi tüm toplumda hissedilmektedir.



Şekil 2. Saldırgan profillerinin yetenek değerlendirilmesi (Ability Assessment of Attacker Profiles)



Şekil 3. Zaman İçerisinde Saldırganların Gelişimi (Development of Hackers in Time)



Şekil 4. 2016 yılında siber saldırı motivasyon istatistiği [8] (Statistics of Cyber Attack Motivations in 2016)

2. SALDIRI AĞACI (ATTACK TREE)

Saldırı ağacı temel olarak belirli bir sistem üzerindeki güvenlik açıklarından faydalanılarak sistemin ele geçirilmesi veya zarar verilmesi sürecinin, ağaç yapılı bir model ile grafiksel olarak gösterilme yöntemidir. Bu teknik kötü niyetli kullanıcılar ve düşmanlardan oluşacak risklerin yönetimi ve değerlendirmesinde etkilidir [9].

Tehdit analizinde sezgisel yaklaşımla ispatlanan saldırı ağacı modeli ilk olarak Schneir [10] tarafından önerilmiştir. Bu model değişen saldırılara bağlı olan sistemlerin güvenliğini tanımlayan resmi ve metodolojik bir yol sunar. Temel olarak kök yaprağı (root leaf) yetkisine erişmek için farklı yollar deneyerek bir sisteme karşı yapılan saldırılar bir ağaç yapısında sunulmuştur.

Saldırı ağacı modeli; gerçek hayatta BGP (Border Gateway Protocol) yönlendirme protokolü [11], akıllı telefonlar üzerinde mobil TAN güvenliği [12], online banka sistemi [13], SCADA sistemleri [14], nükleer kontrol sistemleri [15] ve RFID ağlar [16] gibi sistemler üzerinde kullanılmaktadır. Bu modelle sistemler üzerine gerçekleştirilecek siber saldırılar modellenerek matematiksel olarak saldırının başarılı bir şekilde gerçekleşme olasılığı hesaplanabilir.

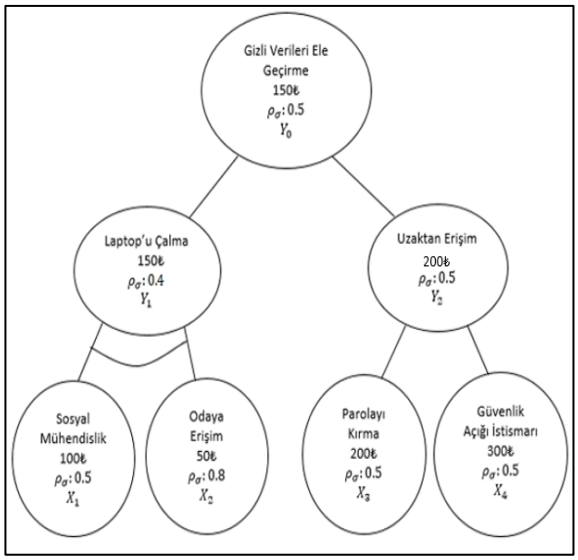
Lenin [17] yaptığı çalışmada üç tür sistem özelliğini ve üç tür saldırgan özelliğini kullanmıştır. Sistem özellikleri; harcamaları, zorlukları ve gerekli minimum saldırı zamanıdır. Saldırgan özellikleri; bütçe, yetenek ve uygun zamandır. Lenin'e göre hesaplamalarda saldırganların saldırılarını başarılı bir şekilde gerçekleştirmek için gerekli parametreler bunlardır. Saldırgan, masraflarını karşılamak için yeterli bütçeye sahip olmalı, sistemdeki zorluğu aşmak için yeterli yeteneğe sahip olmalı ve gerekli minimum zamanı karşılamak için yeterli zamana sahip olmalıdır.

Jurgenson ve Willemson'un yaptığı çalışmada [18], Şekil 4'teki saldırı ağacı kullanılarak Boolean formülüyle X_1, X_2, X_3 ve X_4 değişkenleri tanımlanmış ve bu değişkenler saldırı ağacında soldan sağa doğru Denklem 2'de gösterilmiştir. Buna göre saldırganın amacı bir firmadaki gizli bilgiyi ele geçirmektir. Bu gizli bilgi 2 farklı yolla ele geçirilebilir. Bunlar; laptopu çalmak veya (*OR*) uzaktan erişim sağlamaktır. Saldırgan, laptopu 2 farklı yolla çalabilir. Bunlar; sosyal mühendislikle anahtarı ele geçirme ve (*AND*) laptopun bulunduğu odaya erişimdir. Saldırgan, uzaktan erişim için, gizli bilgileri ele geçirmede diğer bir yol olarak, parolayı kırabilir veya (*OR*) güvenlik açığını istismar edebilir. Denklem 2'de bu durum matematiksel olarak ifade edilmiştir.

$$F = (X_1 \wedge X_2) \vee (X_3 \vee X_4) \quad (2)$$

Verilen örnekte saldırganın gizli bilgileri ele geçirme girişimleri için birçok parametre bulunur. Bu parametrelere maliyet, saldırı başarı ihtimali örnek olarak verilebilir. Parametreyi maliyet olarak

değerlendirmek gerekirse *AND* düğümlerindeki saldırı maliyetleri toplanır, *OR* düğümündeki saldırı maliyetlerinden en az olanı tercih edilir. Örnek olarak sosyal mühendislikle elde edilen anahtar maliyeti 100₺, odaya erişim 50₺, parolayı kırma 200₺, güvenlik açığını istismar etme 300₺ olduğunda; *AND* işlemiyle hesaplanan laptopu çalma 150₺, *OR* işlemiyle hesaplanan uzaktan erişim 200₺ olur. Sonuçta; *OR* işlemiyle hesaplanan gizli verinin ele geçirilmesi 150₺ maliyetinde olur.



Şekil 5. Maliyet ve Başarı İhtimali Açısından Saldırı Ağacı Gösterimi (Notation of Attack Tree in Terms of Cost and Probability of Success)

Aynı örnek saldırı başarısının ihtimali üzerinden değerlendirilecek olunursa; *AND* işlemlerinde iki saldırı girişiminin çarpımı, *OR* işleminde saldırı girişim ihtimallerinden en az olanı tercih edilir. Örnekte *AND* işlemiyle hesaplanan laptopu çalma ihtimali alt yaprakların çarpımıyla 0,4 olarak hesaplanır. *OR* işlemiyle hesaplanan odaya erişim ihtimali ise alt yapraklardan fazla olanı dikkate alınarak 0,5 olarak hesaplanmıştır. Kök yaprağa ulaşırken hesaplanan alt yapraklardan *OR* işlemiyle fazla olan başarı ihtimali tercih edilerek belirlenir.

Saldırı ağaçlarının hesaplamasında üç farklı yöntem kullanılır. Bunlar; birbirine bağlı birçok parametrenin kullanıldığı çok parametreli, saldırı bileşenlerinin sıralaması dikkate alınarak seri model ve karşı önlemlerin olduğu saldırı-defans ağacıdır. Bu çalışmada, saldırganın yeteneğine yönelik matematiksel bir model önerildiğinden çok parametreli ve seri model saldırı ağacı modelleri incelenmiştir. Saldırı-defans modeli ileriki çalışmalarda incelenecektir.

A. Çok Parametreli Saldırı Ağaçları (Multi-Parameter Attack Trees)

Saldırı ağacında birbirine bağlı birçok parametre ayrılmasıyla oluşturulan yöntemdir. Bu yöntemde daha önce bahsedilen [17] çalışmadaki Denklem 1 kullanılmıştır. Her bir saldırı bileşeni "*True*" veya "*False*" olarak denenebilir. Fonksiyon, *True* değerinde dönerse, saldırı ağacında kök düğümüne (Gizli bilgiyi ele geçirme) ulaşılmıştır anlamına gelir. Çok parametreli saldırı ağacı modelindeki temel amaç birçok saldırı vektörünün çıkışını optimize etmektir. Çıkışın optimize edilmesi saldırgan için en fazla çıkışın alınması demektir. Denklem 3'te optimizasyon formülü verilmiştir.

$$\text{Çıkış} = \max\{\text{Çıkış}_\sigma : \sigma \subseteq X, F(\sigma := true) = true\} \quad (3)$$

Denklem 3'te verilen σ saldırı araçlarını, *X* ise giriş saldırılarını simgeler. Çıkış, saldırı araçlarının sadece verilen Boolean formülünün *True* sonucunu verecek şekilde sonuçlanmasından hesaplanır. Bu hesaplamada giriş saldırılarından bir tanesi "*True*" diğerleri "*False*" olarak alınır. Denklem 4'te saldırı aracının çıkışı, kök düğümünün kazanç (gains) değişkeni temel alınarak ve saldırı bileşenlerinin maliyetleri dikkate alınarak hesaplanır.

$$\text{Çıkış}_\sigma = \rho_\sigma \; x \; Kazanç - \sum_{X_i \in \sigma} Masraf_i \quad (4)$$

ρ_σ simgesi saldırının başarı ihtimali olarak gösterilmiştir. Saldırı aracından her bir saldırı bileşeni (X_i) için masraflar toplanmıştır.

Saldırı aracının başarı ihtimali, kök düğümünün ve ara düğümlerin başarı ihtimallerinin hesaplanmasıyla belirlenir. Kök düğümündeki başarı ihtimalinin hesaplanmasında aşağıdaki işlemler takip edilir:

$X_i \notin \sigma$: Başarı ihtimali = 0,

$X_i \in \sigma$: Başarı ihtimali = atanmış kalan değer,

Yapraksız düğümün (*i*) başarı ihtimali = Alt düğümlerinin (*j*) hesaplanmasına bağlıdır.

AND düğümü formülü:

$\prod_{j=1}^{k} p_{i_j}$ (Hepsi başarılı olmalı) (5)

OR düğümü formülü:

$1 - \prod_{j=1}^{k}(1 - p_{i_j})$ (6)

Masraflar, harcamalardan ve cezalardan oluşturulur. Denklem 7'de her bir düğümdeki masraf hesaplaması verilmiştir.

$$Masraf_i = Harcama_i + p_i x \pi_i^+ + \left(1 - p_{i_j}\right) + \pi_i^- \quad (7)$$

- π_i^+: Saldırı başarılı olursa beklenen ceza
- π_i^-: Saldırı başarısız olursa beklenen ceza

B. Seri Model Saldırı Ağaçları (Serial Model Attack Trees)

Çok parametreli saldırı ağacı modelinde, saldırganın gerçekleştireceği saldırıda giriş saldırılarını farklı olmayan bir sıralamayla gerçekleştirdiği düşünülmüştür. Bir veya daha fazla giriş saldırısında başarısız olunması durumunda saldırgan stratejisini değiştirir ve her giriş saldırısı birbiriyle bağlantılı olarak hesaplanır. Seri modelde; giriş saldırıları, kök düğümüne erişmedeki başarı ihtimalini etkilemiyorsa saldırgan herhangi bir giriş saldırısını gerçekleştirmez. Bu durum şu şekilde özetlenebilir; eğer *AND* düğümündeki alt saldırılar başarısız olursa saldırgan herhangi bir *AND* düğümündeki alt saldırıyı gerçekleştirmez veya *OR* düğümündeki alt saldırı başarılı olursa saldırgan diğer *OR* düğümü alt saldırılarını gerçekleştirmez.

Paralel modelde Denklem 3 kullanılırken, seri modelde Denklem 8 kullanılmaktadır.

$$Çıkış_{\sigma} = \rho_{\sigma}\, x\, Gains - \sum_{X_i \in a} p_{a,i} x Masraf_i \qquad (8)$$

Burada a seçilen saldırı aracının permütasyonunu simgeler. Bu ihtimal; saldırganın, eğer bir saldırı kök düğümüne erişme ihtimaline etki etmiyorsa saldırmama ihtimalinden dolayı eklenmiştir.

3. ÖNERİLEN ÇALIŞMA (PROPOSED WORK)

Saldırgan profilinin belirlenmesi, gerçekleştirilecek siber saldırının sistemde yaratacağı etkiyi öngörme açısından çok önemlidir. Bundan dolayı saldırgan profilinin matematiksel formülünün çıkarılması ve sistemlerin buna göre tasarlanması hayati öneme sahiptir.

Pieters ve ark. yaptıkları çalışmalarda [19-21], saldırganın yeteneği ve sistemin zorluğu düşünülerek saldırının başarı ihtimalini, madde tepki kuramını (item response theory) kullanarak Denklem 9'da gösterildiği gibi matematiksel bir ifade şeklinde çıkarmışlardır. Buna göre siber saldırıların gerçekleşme olasılığının hesaplanmasında kullanılan saldırgan profili karakteristiklerini gelir, yetenek ve uygun zaman şeklinde düşünmüşlerdir.

$$P = (e^{\beta-\delta})/(1+e^{\beta-\delta}) \qquad (9)$$

β: Saldırganın yeteneği,

δ: Sistemin zorluğu

Madde tepki kuramına göre; parametreler arasındaki bağımsızlık yeni parametreler eklenmesine imkan vermektedir. Dolayısıyla sunulan bu çalışmada, daha gerçekçi bir sonuç almak için gelir, yetenek ve uygun zaman şeklinde verilen saldırgan profili karakteristiklerine ek olarak saldırgan profili parametreleri daha fazla genişletilmiş ve eğitim seviyesi, bilgi seviyesi, azim ve vatanseverlik şeklinde dört yeni parametre daha eklenmiştir. Önerilen yeni parametrelerin açıklamaları ve önemi aşağıda kısaca verilmiştir. Parametrelerin puanlaması Likert Ölçeği [22] baz alınarak yapılmış ve elde edilen motivasyon ve parametre seviyeleri aşağıdaki Tablolar 1, 2, 3 ve 4'te gösterilmiştir.

Eğitim Seviyesi: Siber güvenlik alanında kişinin teknik eğitim seviyesini gösteren parametredir. Kişinin bu alanda aldığı eğitim seviyesi, gerçekleştireceği siber saldırının etkisini ve başarı oranını etkileyebilmektedir. Matematiksel olarak ifade etmek için eğitim seviyesi Tablo 1'de verilen ölçek kullanılarak puanlanmıştır. Puanlama, kişinin eğitim seviyesiyle sahip olduğu teknik yeterlilikleri ve siber güvenlik farkındalığı düşünülerek yapılmıştır.

2010 yılında tespit edilen Stuxnet solucanını analiz eden araştırmacılar, bu zararlı yazılımın normal bir programcı tarafından yazılamayacağını, içerdiği fonksiyonlar ve etkisi bakımından ancak devlet destekli akademisyen veya çok yetenekli kişiler tarafından yazılabileceğini söylemişlerdir [23]. Bu bakımdan kritik altyapı ve bilgi sistemlerine saldıran kişilerin aldığı eğitim seviyesi, hedef alınan sistemi hangi seviyede etkileyeceğiyle orantılıdır.

Tablo 1. Eğitim seviyesi puanlaması (Grading of Education Level)

Eğitim Seviyesi	Puan
Ortaokul	1
Lise	2
Üniversite	3
Yüksek Lisans	4
Doktora	5

Bilgi Seviyesi: İnternet teknolojisinin gelişmesiyle birlikte bilgiye erişim daha hızlanmış ve saldırganlar bu bilgileri sistemlerin zafiyetlerini sömürmek için kullanmaya başlamıştır. Eğitim seviyesi az olan bir kişi dahi internette Google hacking [24] veya Google dorks yöntemleriyle tehlikeli bilgilere ulaşabilmekte ve sistemlere zarar verebilmektedir.

Basit bir örnekle, 2012 yılının Ocak ve Mart ayları arasında Avusturya'da 15 yaşında bir çocuk 259 firmanın bilgi sistemleri altyapısına sızmaktan tutuklanmıştır. Bu firmaların web sitelerinin ve veri tabanlarının güvenlik açıklarını tarayıp istismar eden çocuk 90 gün boyunca sistemlerde fark edilmeden kalmayı başarabilmiştir. Avusturya polisine ifade veren bu çocuk canının sıkıldığını ve kendisini ispatlamaya çalıştığını söylemiştir. Anti-sosyal olan ve internet dünyasında övgü ve onay kazanmak için Anonymous gibi farklı hacktivist gruplara üye olmuştur. Üye olduğu forumlarda bu çocuğa başarılı saldırılar yapması için internet üzerinde farklı kaynaklar verilmiş ve bu çocuk 3 ay içinde 2000

kişinin üye olduğu forumda en iyi 50 hacker arasına girmiştir. İnternet üzerinde ücretsiz olarak bulunabilen hacking araçlarını kullanan bu çocuk girdiği sistemlerde "ACK!3STX" imzasını bırakmıştır [26]. Bu örnekten görüldüğü üzere; eğitim derecesi düşük olsa bile bilgi seviyesi yüksek olan kötü niyetli bilgisayar kullanıcıları sistemlere zarar verebilmekte ve sızabilmektedir.

Yukarıda açıklanan nedenlerle saldırganın bilgi seviyesi de ayrı bir parametre olarak dikkate alınmalıdır. Bu bağlamda bilgi seviyesinin puanlaması için Tablo 2'de verilen ölçek öngörülmüştür.

Tablo 2. Bilgi seviyesi puanlaması (Grading of Information Level)

Bilgi Seviyesi	Puan
Çok fazla	5
Fazla	4
Orta	3
Az	2
Çok az	1

Azim: Saldırganın motivasyonunda önemli bir parametre olan hedef sisteme zarar verme, bilgileri ele geçirme veya sistemde kalıcı olma azmi saldırının başarıyla sonuçlanmasında önemli bir etkendir. Robin Hood sendromu, siber istihbarat, finansal kazanç veya politik düşüncesini göstermek gibi birbirinden farklı birçok motivasyonu tetikleyen bu parametre ile saldırganın sistemde kalıcı olma ihtimali artar. Azim, saldırı ağacında kök yaprağa ulaşmak için saldırganın gösterdiği çabayı simgelemekte olup Tablo 3'te puanlaması gösterilmiştir.

Tablo 3. Azim seviyesi puanlaması (Grading of Ambition)

Azim Seviyesi	Puan
Çok azimli	3
Azimli	2
Az azimli	1

Vatanseverlik: Siber saldırılarda devletlerin kullandığı saldırganlarda vatanseverlik parametresi önemli bir rol oynar. Ülkeler arasında politik çekişmeler yaşandığında siber saldırıların arttığı gözlenmektedir. Bu kategorideki saldırganlar bu gibi durumlarda önemli etken olabilirler.

ABD Adalet Bakanı Loretta Lynch'in yaptığı açıklamada 2011 – 2013 yılları arasında 7 İranlı hacker grubunun ABD'deki barajlara ve 46 bankaya siber saldırı gerçekleştirdiğini duyurmuştur [27]. Belirtilen tarih aralığında ABD ve İran arasında siyasi olarak ciddi krizler yaşanmakta olduğu düşünüldüğünde, İran'daki bazı vatansever hacker grupların ülkelerini koruma iç güdüsü ile ABD bilgi ve kritik sistemlerine siber saldırı düzenlemiş olmaları değerlendirilebilir.
Bu parametrenin puanlaması oldukça zor olmasına rağmen matematiksel olarak ifade edilmesi için azim ve kararlılık motivasyonları yüksek saldırganların puanı yüksek olarak kabul edilebilir. Buna göre, çalışmada Tablo 4'te ki gibi örnek bir vatanseverlik puanlaması öngörülmüştür.

Tablo 4. Vatanseverlik puanlaması (Grading of Patriotism)

Vatanseverlik	Puan
Çok vatansever	3
Vatansever	2
Az vatansever	1

A. Parametrelerin Normalizasyonu ve Saldırı Başarı İhtimalinin Analizi (Normalization of Parameters and Analyses of Probability of Successful Attack)

Saldırganların saldıracakları sisteme göre karakteristikleri farklılık gösterebilir. Örneğin kritik altyapılara saldıracak bir saldırganın eğitim seviyesi ve vatanseverlik seviyesinin yüksek olma ihtimali daha yüksektir. Çünkü bu sistemler belirli bir bilgi seviyesi gerektirir ve ülkelerin ulusal güvenliğini etkileyebilecek sistemlerdir. Diğer bir ifadeyle hedef sisteme göre karakteristikler farklılık gösterir. Her sisteme özgü her bir parametrenin 0-1 arasında değişen bir ağırlığı olacaktır. Bu nedenle hesaplanacak olan saldırgan profili parametresi için öncelikle normalizasyon yapılması gerekmektedir [25]. Böylece bütün parametreler 0-1 aralığında olacak ve aralarındaki farkın fazla olduğu durumlarda parametreler tek bir düzen içerisinde ele alınarak hepsi aynı denklem içerisinde kullanılabilecektir. Bu bağlamda gerekli normalizasyon işlemi için Denklem 10'da verilen ifade kullanılmıştır.

$$\alpha_N = \left(\frac{\alpha_p - \alpha_{min}}{\alpha_{max} - \alpha_{min}}\right) \quad (10)$$

α_N : Normalize edilen parametre
∂ : Ağırlık
α_p : Normalize edilecek parametre
α_{min} : Minimum parametre değeri
α_{max} : Maximum parametre değeri

Normalizasyon işlemi sonrasında saldırgan profilini hesaplamak için çok nitelikli fayda teorisi (multi-attribute utility theory) [28] kullanılmıştır. Bu amaçla literatürde daha önce sunulan parametrelere ek olarak yukarıda özetlenen parametreler de eklenmiş ve Denklem 11'de verilen ifade ile saldırgan profilinin (σ) hesaplanması ve matematiksel analizi gerçekleştirilmiştir.

$$\sigma = \sum_{N=1}^{k} \frac{\partial * \alpha_N}{k} \quad (11)$$

Denklem 12'de ise çalışmadaki saldırı başarı ihtimalinin hesabında kullanılan ifade verilmiştir. Yukarıda da bahsedildiği üzere alınan parametrelerde sadece saldırganın yeteneği değil aynı zamanda

saldırganın eğitim ve bilgi seviyesi, azmi ve vatanseverliği de kullanılmıştır.

$$P = {(e^{\sigma-\delta})}\Big/{(1+e^{\sigma-\delta})} \quad (12)$$

B. Bulgular ve Değerlendirme (Findings and Assessments)

Bir önceki bölümde açıklanan yeni parametreler kullanılarak saldırının başarılı olma ihtimali Şekil 4'te verilen saldırı ağacına göre tekrar hesaplanmıştır. Örnek hesaplama için saldırgan profili parametreleri Tablo 5'te gösterildiği gibi kabul edilmiştir. Tabloda sunulan kabullenmeler yapılırken örnek hedefin, bir enerji santralinin otomasyonunu kontrol eden SCADA sistemi olduğu varsayılmıştır. Kritik bir altyapı olarak değerlendirilebilecek bu sistemin yapısı karmaşık olmakla birlikte bir siber saldırı sonucu zarar görmesi durumunda ciddi riskler oluşturacağı göz önüne alınmıştır. Bu sebeple bu sisteme ait ağırlık değeri (∂), 0,8 gibi yüksek bir değer olarak alınmıştır.

Tablo 5. Saldırgan profili parametreleri (Parameters of Attacker Profile)

Parametre	Puan	Normalizasyon
Yetenek	4	0,75
Eğitim Seviyesi	4	0,75
Bilgi Seviyesi	5	1
Azim	2	0,5
Vatanseverlik	3	1

Giriş saldırı düğümlerinin başarılı olma ihtimalleri çalışmada verilen parametrelerle ve her düğümün zorluk derecesiyle birlikte Denklem 12'ye göre tekrar hesaplanmış ve Tablo 6'da gösterilmiştir.

Tablo 6. Önerilen çalışmada giriş düğümündeki saldırı başarı ihtimalleri (Probability of Successful Attacks in Elementary Leaf in Proposed Work)

Düğüm	Sistemin Zorluğu	Başarı İhtimali
X_1	0,5	0,535
X_2	0,2	0,608
X_3	0,6	0,51
X_4	0,4	0,56

Giriş düğümündeki saldırı başarı ihtimalinin hesaplanmasından sonra Denklem 2'de verilen Boolean Fonksiyonu'na göre ara ve kök düğümdeki ihtimaller hesaplanmış ve Tablo 7'deki sonuçlar elde edilmiştir. Elde edilen sonuçların daha iyi analiz edilmesi için çalışma literatürde kabul görmüş mevcut bir analiz ile karşılaştırılmıştır. Bu bağlamda, aynı giriş saldırıları ve kök düğümüne sahip bir saldırı ağacı kullanılarak saldırı başarı ihtimali [18]'deki çalışmayla kıyaslanmıştır. Pieters'ın yaptığı çalışmadaki yöntem kullanılarak aynı şartlar altında elde edilen giriş düğümündeki saldırı başarı ihtimali sonucu Tablo 8'de, ara ve kök düğümdeki saldırı başarı ihtimali Tablo 9'da gösterildiği gibidir.

Tablo 7. Önerilen çalışmada ara ve kök düğümdeki saldırı başarı ihtimalleri (Probability of Successful Attacks in Intermediate and Root Leafs in Proposed Work)

Düğüm	Başarı İhtimali
Y_1	0.325
Y_2	0.51
Y_0	0.51

Tablo 8. Pieters'ın çalışmasında giriş düğümündeki saldırı başarı ihtimalleri (Probability of Successful Attacks in Elementary Leaf in Pieter's Work)

Düğüm	Sistemin Zorluğu	Başarı İhtimali
X_1	1	0,5
X_2	0,5	0,62
X_3	1,5	0,38
X_4	2	0,27

Tablo 9. Pieters'ın çalışmasında ara ve kök düğümündeki saldırı başarı ihtimalleri (Probability of Successful Attacks in Intermediate and Root Leafs in Pieter's Work)

Düğüm	Başarı İhtimali
Y_1	0,31
Y_2	0,38
Y_0	0,38

Bu sonuçlar doğrultusunda önerilen çalışmada ara ve kök düğüm saldırı başarı ihtimali 0.51 iken Pieters'ın yaptığı çalışmada 0.38 olarak hesaplanmıştır. Buna göre önerilen çalışmada elde edilen sonuçların gerçeğe daha yakın sonuç verdiği değerlendirilmiştir. Bunun en temel nedeni Pieters'ın yaptığı çalışmada saldırganın yeteneği olarak tek bir parametrenin baz alınarak hesaplama yapılmış olması, saldırgana ait diğer motivasyon özelliklerinin kullanılmamış olmasıdır. Öte yandan önerilen bu çalışmada, Denklem 12'ye değişken olarak eklenecek farklı parametreler, sonucun daha gerçekçi olmasını sağlayacaktır.

4. SONUÇLAR (RESULTS)

Bu çalışmada, risk analizinde önemli bir değişken olan tehdit varyasyonunun detaylı incelemesi yapılmış, saldırgan profili parametreleri analiz edilerek yeni saldırgan profili karakterleri eklenmiş ve bunlar matematiksel olarak ifade edilmiştir. Yeni parametreler, saldırganda olabilecek karakteristik özelliklere, eğitim durumuna ve bilgi seviyesi dikkate alınarak belirlenmiştir. Saldırı ağacı gösterimi ile örneklenerek çıkarılan saldırgan profili üzerinden çok nitelikli fayda teorisi kullanılarak saldırgana ait farklı karakteristik özellikler incelenmiş ve matematiksel fonksiyonların uygulanmasıyla saldırı başarı ihtimali hesaplanmıştır. Hesaplamada, sistemin zorluğu da dikkate alınarak her giriş saldırısı için Madde Tepki Kuramı kullanılmış ve Boolean Fonksiyonuyla kök düğüme ulaşılmıştır. Böylece gerçekleştirilecek siber

saldırıların başarıyla sonuçlanma ihtimalinin daha gerçekçi bir sonuçla elde edileceği ortaya konulmuştur.

Önerilen bu çalışmayla saldırgana ait yaş, cinsiyet, çalışma alanı gibi farklı karakteristik özellikler de eklenerek çok daha gerçekçi sonuçlar da alınması sağlanabilir. Öte yandan, sistemde alınacak güvenlik önlemleri bu çalışmada hesaba katılmamıştır. Bu nedenle, gelecek çalışmalar için saldırı ağaç modellerinden "saldırı-defans modeli" kullanılarak analizlerin yapılması hedeflenmektedir.

KAYNAKÇA (REFERENCES)

[1] H. Takçı, T. Akyüz, A. Uğur, R. Karabağ, İ. Soğukpınar, "Bilgi Güvenliği Yönetiminde Varlıkların Risk Değerlendirmesi İçin Bir Model", Gebze Yüksek Teknoloji Enstitüsü.

[2] B. Karabacak, S. Özkan, "Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi", Ortadoğu Teknik Üniversitesi.

[3] S. Yılmaz, Ş. Sağıroğlu, "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", 6. International Information Security & Cryptology Conference, 2013.

[4] M. Rogers. "A two-dimensional circumplex approach to the development of a hacker taxonomy", Digital Investigation, 3:97-102, 2006.

[5] İnternet: Cyber Threat Source Descriptions, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions, Erişim Tarihi: 20.04.2016.

[6] İnternet: Psychology and the hacker – Psychological Incident Handling, https://www.sans.org/reading-room/whitepapers/incident/psychology-hacker-psychological-incident-handling-36077, 2015, Erişim Tarihi: 20.04.2016.

[7] C. Poulin, "Effectively Using Security Intelligence to Detect Threats and Exceed Compliance", Reboot Conference 2012.

[8] İnternet: January 2016 Cyber Attacks Statistics, http://www.hackmageddon.com/2016/02/16/january-2016-cyber-attacks-statistics/, Erişim Tarihi: 15.07.2016.

[9] R. T. Ingoldsby, "Creating Secure Systems through Attack Tree Modeling", Amenaza Technologies Limited, 2003.

[10] İnternet: Attack Trees, https://www.schneier.com/cryptography/archives/1999/12/attack_trees.html, Erişim Tarihi: 22.04.2016.

[11] C. Marshall, "Attack Trees and Their Uses in BGP and SMTP Analysis", 2008, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.122.3609, Erişim Tarihi: 22.04.2016.

[12] L. Koot, "Security of mobile TAN on smartphones", Radboud Üniversitesi, Fen Bilimleri Fakültesi, Hollanda, 2012.

[13] K. S. Edge, R. A. Raines, M. Grimaila, R. Baldwin, R. Bennington, C. Reuter, "The Use of Attack and Protection Trees to Analyze Security for an Online Banking System", 40th Annual Hawaii International Conference on System Sciences, Ocak 2007.

[14] M. A. McQueen, W. F. Boyer, M. A. Flynn, G. A. Beitel. "Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System", Proceedings of the 39th Annual Hawaii International Conference on System Sciences, Hawaii, ABD, Ocak 2006.

[15] G. Park, C. K. Lee, J. G. Choi, D. H. Choi, Y. J. Lee, K. Kwon, "Cyber Security Analysis by Attack Trees for a Reactor Protection System" In Proceedings of the Korean Nuclear Society (KNS) Fall Meeting, Güney Kore, Ekim 2008.

[16] Dalton II, C. George, "Analysing security risks in computer and radio frequency identification (RFID) networks using attack and protection trees", International Journal of Security and Networks, 5.2-3 (2010): 87-95.

[17] A. Lenin, "Reliable and Efficient Determination of the Likelihood of Rational Attacks", Talinn Üniversitesi, Bilgi Teknolojileri Fakültesi, 2015.

[18] A. Jürgenson, J. Willemson, "Serial model for attack tree computations" Information, Security and Cryptology–ICISC 2009. Springer Berlin Heidelberg, 2009.

[19] W. Pieters, D. Hadziosmanovic, A. Lenin, L. Montoya, J. Willemson, "TREsPASS: plug-and-play attacker profiles for security risk analysis", IEEE Security & Privacy poster abstracts, 2014.

[20] W. Pieters, S. HG Ven, C. W. Probst, "A move in the security measurement stalemate: Elo-style ratings to quantify vulnerability", Proceedings of the 2012 workshop on New security paradigms. ACM, 2012.

[21] A. Florian, W. Pieters, M. Stoelinga, "Quantitative penetration testing with item response theory", Information Assurance and Security (IAS), 2013 9th International Conference on. IEEE, 2013.

[22] F. Karcıoğlu, S. Akbaş, "İşyerinde Psikolojik Şiddet ve İş Tatmini İlişkisi", Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, Cilt: 24, Sayı: 3, 2010.

[23] D. P. Fidler, "Was stuxnet an act of war? decoding a cyberattack", IEEE Security & Privacy 4.9: 56-59, 2011.

[24] İnternet: Google Hacking Database, Exploit-DB, https://www.exploit-db.com/google-hacking-database/, Erişim Tarihi: 25.04.2016.

[25] Y. Dodge, "The Oxford Dictionary of Statistical Terms", The International Statistical Institute

[26] İnternet: 15-year-old arrested for hacking 259 companies, http://www.zdnet.com/article/15-year-old-arrested-for-hacking-259-companies/, Erişim Tarihi: 13.07.2016.

[27] İnternet: 7 Iranians accused of hacking U.S. banks, New York dam, http://www.computerworld.com/article/3048161/security/7-iranians-accused-of-hacking-us-banks-new-york-dam.html, Erişim Tarihi: 10.07.2016.

[28] E. Shelby, W. James, "Risk-based security engineering through the eyes of the adversary", Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, IEEE, 2005.