Çalışmayı referans vermek için:

Enis Karaarslan, "Siber Güvenlik Felsefesine Giriş", Gelişen Teknolojiler ve Hukuk IV: Siber Güvenlik, OnikiLevha, sf 1-24, 2023

SİBER GÜVENLİK FELSEFESİNE GİRİŞ

(INTRODUCTION TO CYBER SECURITY PHILOSOPHY)

Enis Karaarslan[1*]

GİRİŞ

Siber güvenlik, en sade tanımıyla, iletişim ağları üzerinden birbirleriyle iletişimde olan bütün öğelerin güvenliğini içeren bir kavramdır. Günümüzde, IPv6 ağlar ve özellikle nesnelerin interneti (**"IoT"**) cihazlarının yaygınlaşmasıyla çok sayıda ve çeşitli özelliklere sahip cihazlar ağa bağlanmaktadır. Terim çoğunlukla bilginin güvenliği olarak kullanılsa da özellikle siber zorbalık gibi tehditlere karşı insan psikolojisinin korunması unsurunu da içermektedir[2]. Siber güvenlik kavramını tanımlamak için en az beş öznitelik kullanılmaktadır. Bunlar; aktörler, hedef alınan varlıklar (*asset*), motivasyon, hedeflenen varlıklardaki etki ve güvenligi tehdit eden durumların ne kadar zaman sürdüğüdür[3]. Siber güvenlik sürecini daha iyi anlayabilmek adına bu konularda farkındalık geliştirmek gerekir. Bu doğrultuda, kitap bölümünde, güvenlik ve siber güvenliğin arkasındaki temel felsefe ve düşüncelere dair bilgi verilmesi hedeflenmektedir. Siber güvenlik felsefesi hakkında yazılan her metnin eksik ve tamamlanmamış olacağının farkında olarak başlayalım.

---

[1]* Muğla Sıtkı Koçman Üniversitesi, Mühendislik Fakültesi, Siber Güvenlik Anabilim Dalı

[2] VON SOLMS Rossouw\VAN NIEKERK Johan, "From information security to cyber security.", ***Computers & Security,*** 38, 2013, 97-102.

[3] KADİVAR Mehdi, "Cyber-attack attributes.", **Technology Innovation Management Review,** 4, no. 11, 2014.

Siber güvenliği sağlamak için kullanılabilecek birçok önlem bulunmaktadır. Siber güvenlik fiziksel hayattaki güvenlik ile benzerlikler taşır. Bölüm içinde kavramları anlatırken bu iki dünyadan da örnekler verilecektir. Birinci başlıkta bir siber güvenlik senaryosu ile konuya giriş yapılacaktır. İkinci başlık, konu hakkında bildiklerimiz ve bilmediklerimize dair bir kısım olarak tasarlanmıştır. Üçüncü başlıkta veriden bilgiye ve bilgeliğe ulaşma konusu ele alınacaktır. Dördüncü başlıkta ise siber güvenlik felsefesi dört alt başlıkta incelenecektir. Beşinci ve son başlıkta da bölüm genelinde yazılanlara dair bir tartışma ve sonuç aktarımına yer verilmiştir.

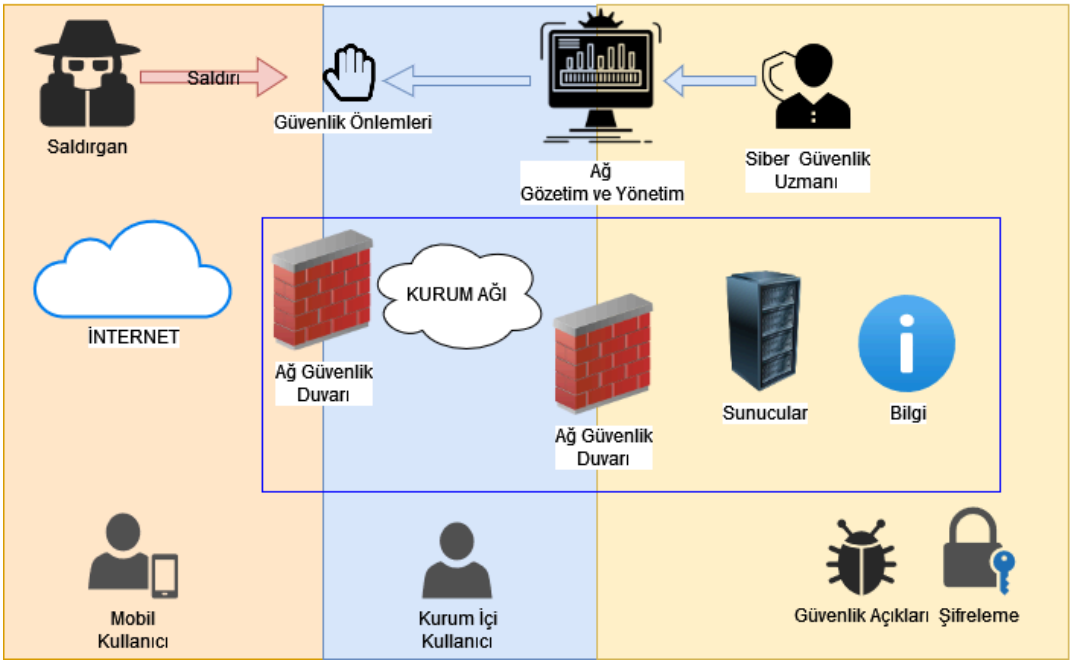
INTRODUCTION:

Cyber security, in its simplest definition, is a concept that includes the security of all items that communicate with each other over communication networks. Today, with the widespread use of IPv6 networks and especially Internet of Things (IoT) devices, many devices with various features are connected to the network. Although the “Cyber security” term is mostly used for information security, it also includes the protection of human psychology against threats such as cyber bullying. At least five attributes are used to define the concept of cybersecurity: actors, targeted assets, motivation, impact on targeted assets, and how long these security-threatening situations last. In order to better understand the cyber security process, it is necessary to raise awareness of these issues. In this direction, it is aimed to give information about the basic philosophy and thoughts behind security and cyber security in the book chapter. Let us start by being aware that any text written about cybersecurity philosophy will be incomplete.

Many measures can be used to ensure cyber security. Cybersecurity has similarities with security in physical life. While explaining the concepts in the chapter, examples from both worlds will be given. In the first section, the subject will be introduced with a cybersecurity scenario. The second section is designed as a part of what we know and do not know about the subject. The third chapter will discuss the issue of accessing knowledge and wisdom from data. The fourth section will examine the philosophy of cyber security under four subtitles. In the fifth and last section, there is a discussion and conclusion about what is written throughout the chapter.

I. SİBER GÜVENLİK SENARYOSU

Güvenlik felsefesine değinmeden önce, siber güvenliğin temellerinin verilebilmesi için bir kurumun siber güvenlik sürecindeki temel aktörleri Şekil 1'de en sade haliyle gösterilmiştir. Bilgisayar ağları her geçen gün daha karmaşık hale gelmektedir. Örneğin; kurum ağları farklı ülke veya şehirlerdeki şubelerden ve bu birimlerin ana merkeze ve bulut altyapılarına olan bağlantılarından oluşmaktadır. Bu birimlerin birbirleriyle iletişimi telekomünikasyon altyapıları üzerinden gerçekleşmektedir.



Şekil 1. Siber Güvenlik Senaryosu

Kurumların bilgi sistemlerine farklı kullanıcı grupları erişim sağlamak isteyecektir. Farklı kullanıcıları; kurum ağlarının içinden bağlanan personel, internet üzerinden bağlanan mobil personel ve dış kullanıcılar olarak gruplayabiliriz. Bu dış kullanıcılar müşteriler olabileceği gibi ortak çalışılan şirketler veya sistemlere izinsiz ulaşmaya çalışan kişiler de olabilir.

Sistemlere izinsiz erişim sağlamaya çalışan kişiler; "*hacker*", "*lamer*", izinsiz giren (*intruder*) veya saldırgan (*attacker*) olarak farklı şekillerde adlandırılmaktadır. "*Hacker*" kavramı gündelik hayatta saldırgan anlamında kullanılmakla birlikte, aslında bir işi çok iyi bilen üstat kişi anlamını taşımaktadır. *McKenzie Wark*'a göre bu kavram MIT elektronik laboratuvarlarında öğrencilerin yaramazlıkları (*prank*) ile başladı[4]. Steven Levy'in de

[4] WARK McKenzie, "A hacker manifesto [version 4.0]", ***Subsol**, 2004,* http://subsol.c3.hu/subsol_2/contributors0/warktext.html (Erişim Tarihi: 05.10.2022)

belirttiği üzere; "*Bir 'hack' olarak nitelendirilmek için, başarının yenilik, stil ve teknik ustalıkla dolu olması gerekir.*"[5]. Alanda, "lamer" veya "script kiddie" gibi lakaplar ise bir uzmanlığı olmamasına rağmen bir başkasının hazırladığı kaynak kodları kullanarak sistemlere giren ve bununla övünen kişiler için kullanılmaktadır. Bu bölümde; siber güvenlikte saldırı yapan kişileri tanımlamak için "saldırgan" kavramı tercih edilecektir.

Teknolojiye hâkim saldırganlar genelde yakalanmadıkları için tanınmazlar. Saldırganlar arasında bireysel çalışanlar olduğu gibi bir grubun parçası olmak da oldukça yaygındır. Bunların arasında "*Anonymous*" gibi politik amaçlı hacktivist olarak tanımlanan gruplar da bulunmaktadır[6]. Öte yandan, saldırgan kurum dışından olabileceği kadar kurum içinden de olabilir. Bununla beraber saldırganın bir birey olması da şart değildir; otonom bir kod veya yapay zeka destekli bir kod olma ihtimali de vardır. Saldırgan dünyanın herhangi bir yerinden siber saldırıyı başlatabilir ve bunu tam olarak nereden başlattığını da belirlemek zordur. Böyle durumlarda, saldırgan farklı ülkeler ve farklı ağlardan ele geçirdiği çeşitli bilgisayar sistemlerini kullanır. Bunu gerçekleştirirken de kendi makinesinden önce bir sisteme, o sistemden bir başka sisteme ve bunu tekrarlayarak farklı diğer sistemlere bağlanır. Saldırıyı son bağlandığı sistem veya sistemler üzerinden gerçekleştirdikten sonra da bütün sistemlerden dijital ayak izlerini siler.

Saldırgan, erişim izni olmayan veriye ve sistemlere ulaşabilmek için ilk aşamada sistemlere sızmaya (*intrusion*) çalışır. Bu durum, bir hırsızın kendine ait olmayan bir eve izinsiz girmesine benzetilebilir. Saldırgan sistemlere sızmak için sistemlerde var olan güvenlik açıklarını kullanır. Bu güvenlik açıkları sistemlerdeki yazılım hatalarından veya yanlış yapılandırmalardan kaynaklanmaktadır. Saldırgan nüfuz ettiği sistemlerdeki verilerin bir kopyasını da genellikle kendisine alır ve onların içeriklerine erişmeye çalışır. Sistemdeki verileri silebilir veya değiştirebilir. Sistemleri çalışamaz hale getirebilmesi de olasıdır. Bunun yanı sıra; sisteme herhangi bir zarar vermeyi tercih etmeyebilir, sadece sistemlere göz atıp çıkabilir. Öte yandan, siber saldırganın sadece sistemin iç işleyişini görüp hiçbir şeye dokunmadan ve veri almadan sistemden çıkması bile gelecekte çeşitli güvenlik problemlerine neden olabilir.

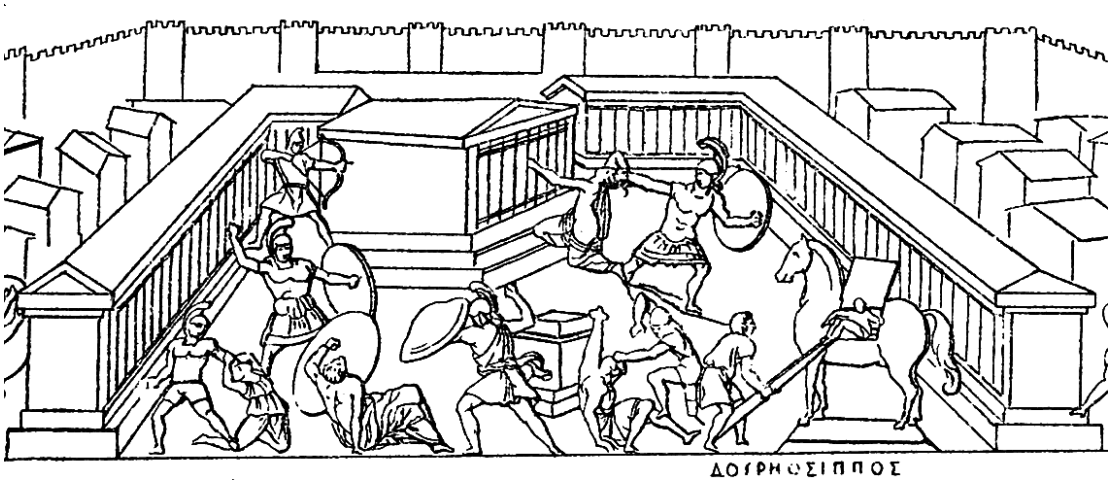
---

[5] LEVY Steven, "*Hackers: Heroes of the computer revolution"*, Vol. 14. Garden City, NY: Anchor Press/Doubleday, 1984.
[6] GOODE Luke, "Anonymous and the political ethos of hacktivism.", **Popular Communication,** 13, no. 1, 2015, 74-86.

Bu bağlamda, siber güvenlikte en önemli dayanağımız kriptoloji (*cryptography*) bilimidir. Eğer veriler kriptoloji teknikleri ile şifrelenmiş ise (*encrypted*); saldırganın kullanılan şifreleme anahtarlarına erişimi olmadığı sürece, ele geçirdiği verilerin içeriğine ulaşması mümkün olmayacaktır. Şifre kırma teknikleri ile veriyi kırması için ise büyük miktarda işlemci gücüne ve uzun süreye ihtiyaç duyacaktır.

Siber güvenlik uzmanı; ağ güvenlik duvarı, nüfuz/saldırı tespit/engelleme sistemleri, antivirüs sistemleri gibi çeşitli önlemleri etkin bir şekilde konuşlandırır (*deploy*) ve yönetir. Bu yöntemlerle saldırıların bir kısmını engellemeye veya etkilerini azaltmaya çalışır. Bu süreçte; bilgisayar ağını, ağ üzerindeki sistemleri ve kullanıcıları sürekli olarak gözlemesi (*monitoring*) ve neyin normal neyin anormal bir etkinlik olduğunun farkına varması gerekir. Böylelikle, herhangi bir saldırı tespiti durumunda uygun önlemi almada zorluk çekmeyecektir.

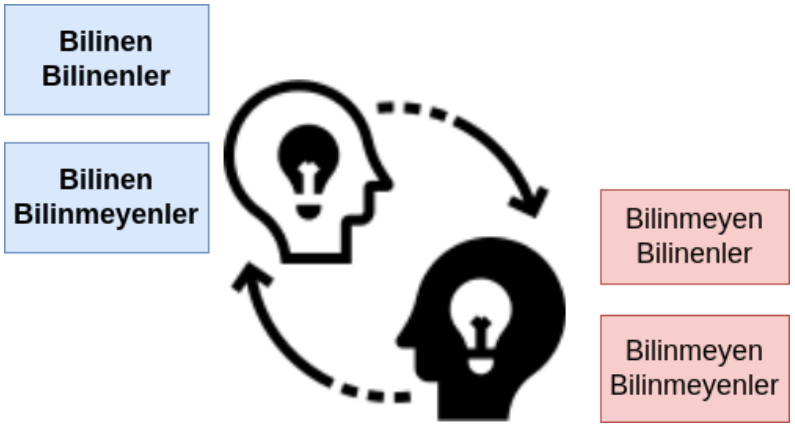
En temel seviyede alınan güvenlik önlemi, ağ güvenlik duvarları (*network firewall*) kullanarak ağa gelen (*inbound*) ve ağdan dışarı çıkan (*outbound*) iletişimleri denetim içinde tutmaktır. Gerçek hayatta kapıda (*gate*) güvenlik kontrolü yapılır. Havalimanı girişlerindeki güvenlik kontrolleri veya bina güvenlik kontrolleri buna örnek olarak verilebilir. Bu gibi önlemler önemlidir fakat tam anlamıyla yeterli oldukları da söylenemez. *İlyada* destanında detaylı bir şekilde bahsi geçen efsanevi Truva atı (bkz. Şekil 2) örneğindeki gibi, savaş sırasında, *Athena*'ya adak olduğu iddia edildiği için atın ve dolayısıyla onun içerisine gizlenmiş Yunan askerlerinin şehir kapısındaki güvenlik duvarını rahat bir şekilde atlatıp içeri sızabilmeleri mümkün olmuştu. Siber güvenlikte de durum böyledir. Kapıda güvenlik kontrolünün yeterince yapıl(a)mamasının en önemli nedeni ise bu gibi kontrollerin ciddi zaman alıyor olması ve kişilerin kontrol süreçlerini neredeyse durma aşamasına getirebilmesidir. Bu nedenle, havalimanlarındaki güvenlik birden fazla kontrol noktasıyla desteklendirilerek sağlanmaya çalışılır. Alana ilk girişte çok detaylı bir kontrol yapılmaz, hızlıca temel kontroller yapılır. Fakat, uçağa yaklaştıkça güvenlik denetimlerinin yoğunluğu kademeli olarak artırılır. Siber güvenlik için bilgisayar ağlarında da benzer mimariler uygulanmakta ve denetimleri yapan ağ güvenlik duvarları benzer şekilde kullanılabilmektedir. Örneğin, sunucuların bulunduğu ağın önüne ikinci bir güvenlik duvarı konulabilir (bkz. Şekil 1). Ayrıca kurumun her şubesine ek bir güvenlik duvarı konumlandırılabilir. Böylece daha etkin çalışan güvenlik sistemlerine ulaşılabilir.



Şekil 2. Truva (Troya) Savaşı ve Truva Atı[7]

II. BİLİNENLER VE BİLİNMEYENLER[8]

Bir şeyi anlamak ve onun hakkında fikir yürütebilmek için önce bilmek gerekir. Şekil 3'de gösterildiği üzere, bazı şeyleri biliyoruz, öte yandan, bazı şeyleri de bilmiyoruz. Dahası, bazen bildiğimizin farkında olabildiğimiz gibi, bilmediğimizin farkında olmadığımız durumlar da bulunacaktır. Siber güvenlik söz konusu olduğunda ise bilmemiz gereken şeyler sabit değildir. Aksine, her yeni teknoloji ve o teknolojinin farklı kullanım şekillerinden dolayı sürekli bir değişim içerisindedir.



Şekil 3. Bilinen ve Bilinmeyenler

Siber güvenlik alanındaki bilgileri sırasıyla dört alt başlıkta incelememiz mümkündür:

---

[7] https://commons.wikimedia.org/wiki/File:Tabula_iliaca_-_Iliupersis.png, 23.8.2022 tarihinde erişim sağlandı
[8] Bu bölümde aksi belirtilmedikçe yararlanılan kaynak: KAĪ XİN Thia, "Lion, zebras and big data anonymization", **Slideshare**, 02.10.2013, https://www.slideshare.net/KaiX/lions-zebras-and-big-data-anonymization (Erişim Tarihi: 05.10.2022)

- Bildiklerimiz
- Keşfetmemiz gerekenler
- Farkında olmamız gerekenler
- Hazır olmamız gerekenler

1. **Bildiklerimiz**

Bilebileceğimiz her şeyi bilgi sistemlerinden toplamak ve analiz etmek durumundayız. Bunlara örnek olarak aşağıdakilerin verilmesi mümkündür:

- Sahip olduğumuz kaynaklara (sistemler, veriler) dair ayrıntılı bilgi
- Kimlerin hangi kaynaklara erişim izni olduğu
- Verilerin nasıl paylaşıldığı
- Verinin kurum ve müşteriler için önem ve değeri
- Kullanım politikaları
- Kanunlar, standartlar ve yönetmelikler

2. **Keşfetmemiz gerekenler**

Riski azaltmak için keşfetmemiz gereken şeyler hakkında da bir öngörümüz olmalıdır. Örneğin; erişim haklarını kötüye kullanabilecek birilerinin var olup olmadığına dair bir fikrimiz olmalıdır. Kurumumuza yapılacak saldırılarda yer alanların motivasyonlarını keşfetmemiz gerekir. Kurum verileri başkalarının eline geçerse oluşabilecek zararlara dair hesaplamalar önceden yapılmalıdır.

3. **Farkında olmamız gerekenler**

Farkında olmamız gereken esas durum gerçeklerdir. Farklılıklar olabilmekle birlikte, bazı temel gerçeklerden söz etmek mümkündür. Kullanıcılarda güvenlik süreçlerini ciddiye almama eğilimi bulunmaktadır. Bilgi paylaşımı ancak gerektiği zaman gerçekleştirilmeli ve sadece ihtiyaç duyulan kadar bilgi aktarılmalıdır. Ayrıca, veri politikaları, kanunlar, standartlar ve yönetmeliklerin sürekli güncellenmesi gerektiğinin farkında olmamız gerekir.

4. **Hazır olmamız gerekenler**

Hazır olmamız gerekenler ise bilinmeyen bilinmeyenlerdir (*unknown unknowns*). Bunun için sürekli olarak sistemlerimizi olağan dışı etkinliklere karşı takip etmemiz gereklidir. Saldırgan

tuzağı (honeypot) sistemleri ve bunları barındıran iç ağlar (*honeynet*) gibi sistemlerin kurulumu ve anlık takibi ile yeni saldırılar hakkında bilgi edinilmesi mümkündür.

III. VERİDEN BİLGİYE VE BİLGELİĞE ULAŞMAK

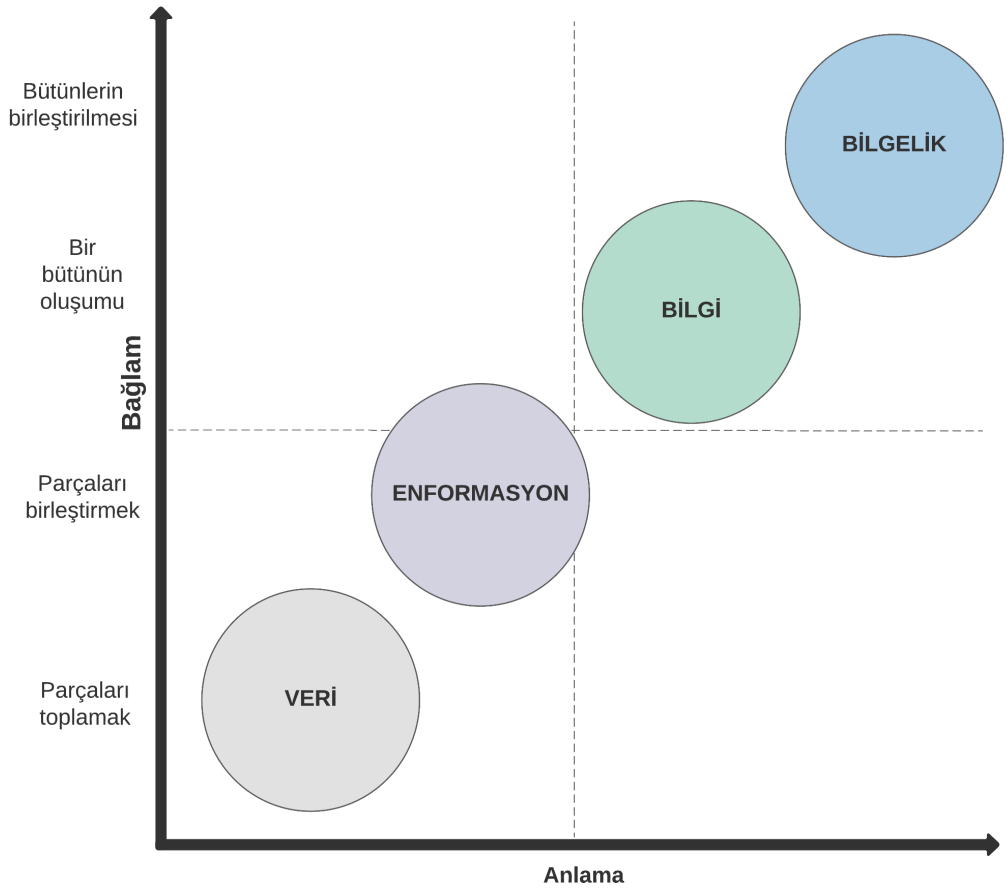
"Bilgeliğe aç kalırken bilgi içinde boğuluyoruz.
Dünya bundan böyle sentezleyiciler tarafından yönetilecek,
doğru bilgiyi doğru zamanda bir araya getirebilen,
onun hakkında eleştirel düşünebilen
ve önemli seçimleri akıllıca yapabilen insanlar."
Edward Osborne Wilson

Francis Bacon, İngiltere'nin Avrupa Rönesansı ile çoktan tanıştığı bir dönemde, 1597 senesinde yayımlanan *Büyük Yeni Düzen* adlı eserinde şöyle demişti: "*Bilgi güçtür*" (*Knowledge is power*). Bu söz aynı zamanda bir üstat (*hacker*) mottosudur. Eserleri bir çok girişimci ruhu etkileyen kişisel gelişim uzmanı *Dale Carnegie* da: "*Bilgi uygulanana kadar güç değildir*" diyerek bu görüşün önemli bir aşamasına dikkat çekmiştir.

Jonathan Hey'in çalışmasında[9] veriden bilgeliğe giden yol işlenmiştir ve Şekil 4'de özetlenmiştir. Siber güvenlik tehdit istihbaratı da benzer şekillerde toplanan verilerden bilgi edinmeye ve duruma dair bir bilgeliğe ulaşmaya giden bir süreci kapsamaktadır. Veri ham gerçektir ve tek başına bir anlam ifade etmez. Verinin anlamlı bir enformasyona dönüşmesi için önce toplanması ve işlenmesi gerekecektir. Toplanan verileri anlamlandırmak için öncelikle sistem ve ağ farkındalığına sahip olmak gerekecektir[10]. Veri filtreleme ve temizleme olarak adlandırılan süreçlerde gereksiz kısımlar çıkarılır. Bu enformasyonların analizi ile bilgi edinilir. Farklı kaynaklardan edinilen bilgilerin analiz edilerek bir araya getirilmesi, kavranması ve duruma uygun çeşitli kriterler sayesinde değerlendirme sürecinden geçmesi ile bilgeliğe ulaşmak hedeflenir. Siber güvenlik uzmanı, sahip olduğu bilgi ve deneyim ile toplanan bilgilerden bir karar verme sürecinde aktif yer alacaktır. Daha hızlı tespit yapmak ve herhangi bir detayı gözden kaçırmamak için yapay zekâ teknolojilerinden yararlanması da faydalı olacaktır.

---

[9] HEY Jonathan, "The data, information, knowledge, wisdom chain: the metaphorical link." **Intergovernmental Oceanographic Commission**, 26, 2004, 1-18.
[10] KARAARSLAN Enis, "Web saldırı saptama sistemlerinin etkinleştirilmesi için sistem farkındalığı ve çok katmanlı güvenlik önlemlerinin gerçekleştirilmesi", Doktora Tezi, **Ege Üniversitesi Fen Bilimleri Enstitüsü**, 2008.



Şekil 4. Veri Enformasyon Bilgi Bilgelik Hiyerarşisi[11]

Jonathan Hey 2004 senesinde yazdığı bu çalışmasında[12], bilgi ve verinin sensörlerle toplanıp kablosuz iletilmesini örnek vererek; günün birinde "enformasyon alanı" veya etrafımızdaki bilgileri nefesle alıp alamayacağımızı sorgulamıştır. Geçen zaman içinde bu dedikleri henüz bu kapsamda gerçek olmamış olsa bile günümüzde siber güvenlik ile ilgili birçok verinin güvenlik operasyon merkezlerinde (**"SOC"**) toplanarak etkin yönetimi mümkün olmaktadır. SOC siber güvenliği sağlamak için en önemli yapı taşlarından birisidir. Lakin bu merkezlerde kullanılabilecek birbiriyle entegre araçlar az sayıdadır, otomasyonun seviyesi henüz yetersizdir ve standartlar bulunmamaktadır[13].

---

[11] Jonathan Hey'in çalışmasından esinlenmiştir; HEY Jonathan, "The data, information, knowledge, wisdom chain: the metaphorical link." **Intergovernmental Oceanographic Commission**, 26, 2004, 1-18.
[12] HEY Jonathan, "The data, information, knowledge, wisdom chain: the metaphorical link." **Intergovernmental Oceanographic Commission**, 26, 2004, 1-18.
[13] SHAHJEE Deepesh/WARE Nilesh, "Integrated Network and Security Operation Center: A Systematic Analysis.", **IEEE Access**, 10, 2022, 27881-27898.

IV. SİBER GÜVENLİK FELSEFESİ

Siber güvenlik felsefesine dair temel önermeler aşağıdaki alt başlıklarda işlenecektir:

- Güvenlik açıkları
- Saldırı / nüfuz
- Temel önermeler
- Güvenlik algısı
- Güvenlik süreci
- Ahlak; Suç ve Ceza

Konular ilgili alt bölümlerde ayrıntılı olarak ele alınacaktır.

1. Güvenlik Açıkları

"Eğer bu kadar kötü yazılım güvenliğine sahip olmasaydık,
bu kadar çok ağ güvenliğine ihtiyacımız olmayacaktı."
Bruce Schneier, kriptograf

Sistemlerdeki yazılımlarda çeşitli güvenlik açıkları/zafiyetleri (*vulnerability*) bulunmaktadır. Bunlar çoğunlukla geliştirme süreçlerinde yazılımların güvenli kodlama (*secure coding*) pratiklerine dikkat edilmemesi veya yanlış yapılandırmalardan kaynaklanır. Güvenlik araştırmacıları, bir yazılımdaki güvenlik açıklarını bulduklarında bunu firmalara veya topluluklara (*community*) rapor ederler. Bunların birçoğu MITRE CVE (https://cve.mitre.org/) gibi herkese açık veritabanlarında yayınlanır. Bunun yanı sıra, raporlanmayan ve karanlık ağda (*dark web*) satılan güvenlik açıklarının da olduğu bilinen bir gerçektir.

Güvenlik açıkları öğrenildikten sonra; saldırganlar bu açıktan yararlanacak kodları (*exploit*) yazarken, firmalar ya da özgür yazılım toplulukları bu açığı kapatacak yama (*patch*) geliştirirler. Yama geliştirme süreci gecikebilir veya ihmal edilebilir. Sıfırıncı gün saldırıları (*zero-day attack*) bu güvenlik açıklarına önlem alınmadan önce gerçekleştirilen girişimlerdir. Geliştirilen yama duyurulduktan sonra da tehdit tam anlamıyla bitmiş sayılmaz. Bu durumun başlıca nedeni de yamanın dünya çapında ilgili bütün sistemlere uygulama aşamasında gecikme yaşayacağı gerçeğinden kaynaklıdır.

2. Saldırı

Herkes siber saldırı yapabilir ve her siber sistem saldırıya uğrayabilir. Bu saldırının ilk basamağı bir bilgi sistemine yetkisiz giriş hakkı kazanma (nüfuz etme/sızma) işlemidir. Saldırılar aktif veya pasif olabilir. Pasif saldırılar sadece bilgi edinmek amaçlı iken aktif saldırılarda bilgi ve sistemler üzerinde değişiklik(ler) gerçekleştirilir. Saldırganların sistemlere erişim sağlamak için kullanabileceği çeşitli yol ve yöntemler bulunmaktadır. Bunların hepsine birden saldırı vektörü denir. Bir siber saldırıda birden fazla saldırı vektörü kullanılabilir. Bir siber saldırı kısa veya uzun zaman sürebilir. Örneğin; 2007 senesinde TJX şirketlerine düzenlenen saldırının otuz iki hafta sürdüğü kayıtlara geçmiştir[14]. Şayet saldırı bir sızma şeklinde gerçekleştiyse, yetkililerin olaydan (*incident*) ancak uzun süre sonra farkına varabilmesi ihtimali de vardır. Radisson Otel grubundaki güvenlik ihlalinin ancak haftalar sonrasında yetkililer tarafından fark edilmesi bu duruma örnek olarak verilebilir[15].

Bir sistemin sahip olduğu her servis saldırganların kullanabileceği yeni bir saldırı yüzeyi anlamına gelir, tıpkı bir binaya birden fazla noktadan giriş olabilmesi gibi. Bu nedenden ötürü, gereksiz servisleri kaldırma veya kısıtlama yöntemleriyle saldırı yüzeyinde azaltmaya gitmek önemlidir.

Siber saldırı da olsa, olayın bir kısmı fiziksel dünyada gerçekleştirilebilir. Bu nedenle, ilk etapta fiziksel güvenliği sağlamaya öncelik verilmelidir. İnsanın bilindik davranış şekillerini kullanan sosyal mühendislik saldırılarına (*social engineering attack*) yönelik kullanıcıları bilinçlendirmek de kritik önem taşımaktadır.

Siber nüfuzları izlemek ve analiz etmek için çeşitli yaklaşımlar bulunmaktadır. Bunların başlıcaları siber ölüm zinciri (*cyber kill chain*), elmas modeli ve MITRE ATT&CK çerçevesidir. 2011 senesinde Amerikan Savunma Bakanlığı siber uzayı da bir savaş alanı olarak tanımlamıştır. *Lockheed Martin* firması da siber saldırıları tanımlamak için siber ölüm

---

[14] KADİVAR Mehdi, "Cyber-attack attributes.", **Technology Innovation Management Review,** 4, no. 11, 2014.
[15] PAGANİNİ Pierluigi, "The hotel chain Radisson Hotel Group suffered a security breach that exposed personal information of the members of its loyalty scheme.", **Security Affairs**, 31.10.2018, https://securityaffairs.co/wordpress/77530/data-breach/radisson-hotel-group-data-breach.html (Erişim Tarihi: 05.10.2022)

zinciri diye adlandırılan bir model ortaya koymuştur[16]. Bu model bir siber saldırının olası aşamalarını göstermektedir. Bu aşamalar şu şekilde sıralanmaktadır[17]:

1. Keşif (*Reconnaissance*): Sistem öğelerinin ve güvenlik açıklarının tespiti,
2. Silahlandırma (*Weaponize*): Siber silah (cyber weapon) diye de tanımlanan araçların hazırlanması,
3. Gönderim (*Delivery*): Siber silahın hedef ortama taşınması,
4. Açıkları kullanmak (*Exploitation*): Siber silahın hedef sistemde çalıştırılması,
5. Kurulum (*Installation*): Sistemde kalıcılığı sağlamak için arka kapıların kurulması, var olan zayıflıkların yamanmasıdır ve böylelikle başka bir saldırganın sistemi ele geçirmesinin de önlenmesi,
6. Komuta ve kontrol (*Command and Control*): Sunucular aracılığı ile ele geçirilen sistemlerin yönetiminin sağlanması,
7. Amaca göre hareket (*Actions on Objectives*): Saldırganın amacına göre sistemlerin kullanılmasıdır.

Amerikan Savunma Bakanlığı, sızma analizi için 2013 senesinde elmas modelini önerse de günümüzde MITRE ATT&CK (https://attack.mitre.org/) çerçevesi[18] yaygın olarak kullanılmaktadır. Bu çerçeve ile gelişmiş kalıcı tehditler (**"APT"**) ve saldırganların kullandığı taktikler, teknikler ve prosedürler (**"TTP"**) modellenmektedir. Bu çerçeve aynı zamanda örnekler, tespit ve engellemeye (mitigate) dair ayrıntılı bilgiler de barındırmaktadır.

3. Temel önermeler

Her şeyden önce siber güvenlik farkındalığı (*awareness*) gereklidir. Sistemi kullanan herkesin tehditlerden haberdar olması ve buna göre gereken önlemleri alması için bilinçlendirme ve eğitim çalışmaları yapılmalıdır. Bu aşamada oyunlaştırma (*gamification*) kullanılabilir.

Şimdi geçerli olan bir güvenlik önlemi, sonrasında geçerliliğini yitirebilir. Örneğin; asimetrik şifreleme halen aktif kullanılmaktadır ama kuantum bilgisayarların daha yaygın kullanımına

[16] CYCRAFT, "CyCraft Classroom: MITRE ATT&CK vs. Cyber Kill Chain vs. Diamond Model", **Medium**, 01.07.2020, https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f (Erişim Tarihi: 05.10.2022)

[17] Yadav, Tarun, and Arvind Mallari Rao. "Technical aspects of cyber kill chain.", In International symposium on security in computing and communication, Springer, Cham, 2015, 438-452.

[18] STROM Blake E., Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. "Mitre att&ck: Design and philosophy.", In Technical report. The MITRE Corporation, 2018.

başlanmasıyla artık kullanılan şifrelerin kırılması mümkün olacağından bu yöntem geçerliliğini yakın gelecekte yitirecektir.

Her şeye uyan bir şablon yapı yoktur. Örneğin; kritik altyapıların (*critical infrastructure*) güvenliğinde farklı seviyede, ev kullanıcıları veya mobil kullanıcılar için ise farklı seviyelerde güvenlik önlemi gereklidir. Her farklı altyapının ve kullanıcı türlerinin farklı karakteristik özellikleri ve buna bağlı farklı kullanım politikaları olacaktır. Bunların analiz edilmesinin ardından uygun önlemlerin konumlandırılması gereklidir.

Güvenlik ve kullanışlılık ters orantılıdır. Güvenlik önlemleri ne kadar artırılırsa, kullanıcılar o sistemi kullanmakta o kadar zorlanacaktır. Bu yüzden, güvenlik önlemleri ve kullanışlılık bir denge içerisinde olmalıdır. Öte yandan, güvenlik gerekliliğine göre bir özelliğe öncelik de verilebilir. Örneğin; mobil siber ağlarda kullanıcıların sistemi rahatlıkla kullanabilmesine öncelik verilir. Enerji ve telekomünikasyon hatları gibi günlük yaşamın devamını mümkün kılan kritik altyapılarda sistemin ayakta kalması önem taşıdığından dolayı güvenliğe öncelik verilir.

Veriyi korumak için ilgili güvenlik servisleri hedeflenir. Gizlilik (*confidentiality*), bütünlük (*integrity*) ve erişilebilirlik (*availability*) ("**CIA**") temel güvenlik servisleri sağlanmalıdır. Gizlilik; bilginin herkes tarafından erişilememesi, sadece o veriye erişimine izin verilenler tarafından okunabilmesidir. Bütünlük; bilginin aslı gibi kalmasıdır. Bu da izin verilen kişiler/sistemler dışında bir başkası tarafından değiştirilmesinin engellenmesi ile sağlanır. Erişilebilirlik; ilgili servislerin her an çalışır olması ve bilginin erişilebilir bir şekilde bulunmasıdır. Bu güvenlik süreçlerinin geçerli olması için kimlik doğrulama (*user authentication*), yetkilendirme (*authorization*) ve veri mahremiyeti (*privacy*) gibi başka güvenlik servislerinin sağlanması da gerekebilecektir. Güvenlik denince akla öncelikle gizlilik gelmekle birlikte, günümüzde veri bütünlüğü gitgide daha önemli bir hale gelmektedir. Bir verinin değişmediğini garanti etmek için ilgili verinin bir nevi gölgesini tutan "*hash*" fonksiyonlarına dayanan sistemler yoğun bir şekilde kullanılmaktadır. Bu yapıların kullanılmasıyla güvene (*trust*) dayanan merkeziyetsiz (decentralized) çözümler yoğun bir şekilde kullanılmaya başlanmıştır[19].

[19] KARAARSLAN Enis/AKBAŞ M. F. "Blokzinciri tabanlı siber güvenlik sistemleri", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, 3(2), 2017, 16-21.

Mükemmel güvenlik önlemlerine yaklaşabilmek için kullanabileceğimiz sınırsız bütçeler yoktur. Bu yüzden, güvenlik uzmanları ellerindeki kısıtlı bütçe ile en riskli buldukları alanlar için güvenlik önlemlerini konumlandırır (*deploy*). Yapılacak güvenlik harcamaları korunacak varlıkların değerinden fazla olmamalıdır. Fakat, buna bir istisna olarak itibarın oldukça önemli ve değerli olduğunu da hatırlatalım. Örneğin; bir web sitesi bir ilan panosu gibidir, ele geçirilmesi önemli değildir. Tabii ki bu önerme, web sitesinde gizli bir bilgi bulundurulmadığı veya o sistem üzerinden diğer kritik sistemlere erişim sağlanamadığı sürece geçerlidir. Yine de bir güvenlik firmasının web sayfasının ele geçirilmesi, o firma için çok ciddi bir itibar kaybına yol açacağından dolayı web sitesinin güvenliği önem kazanmaktadır.

Fiziksel dünyada yüzde yüz güvenlik olmadığı gibi, siber dünyada da yüzde yüz güvenlikten söz edilemez. Alınan bütün güvenlik önlemleri aslında saldırganın işini zorlaştırmak ve zaman kazanmak içindir. Bu süreç içerisinde, esas hedef, saldırıların tespit edilmesi ve elde edilen tespitler sonucunda gereken önlemlerin alınmasıdır.

4. Güvenlik Algısı

Siber ortamda, sürekli güvende olunduğuna dair bir algı yanlıştır. Farkında olunmalıdır ki her şey saldırıya uğrayabilir ve bunun sonucunda ele de geçirilebilir, çünkü yüzde yüz güvenlik diye bir şey yoktur. Bir zincir ancak en zayıf halkası kadar güçlüdür.

Gerçek hayatta “Dikkat köpek var” gibi tabelalarla saldırgan uyarılır. Buradaki asıl amaç saldırganı uzaklaştırmaktır. Aynı şekilde, siber sistemlerin arayüzlerinde sistemin sürekli takip edildiğine dair uyarılar verilmelidir.

Temel önermelerde de söz ettiğimiz üzere saldırganın işini zorlaştırmak için güvenlik önlemlerinin arttırılması gerekir. Güvenliği güçlendirmek için birden fazla zincir, birden fazla güvenlik önlemi alınabilir. Buna çok katmanlı güvenlik (*multi-layer security*) denir. Şekil 5’teki kumdan kale örneğinde de temsili olarak görüldüğü üzere; fiziksel hayattaki kaleler hep bu mimaride yapılmıştır. Bu kalelerin güvenliği çevrelerine açılan hendekler, kuleler ve benzeri birçok güvenlik önlemleri ile desteklenerek arttırılırdı. Saldırgan bir suru aştığında savunma kuvvetleri bir iç sura geçerek savunmayı devam ettirirdi. Kumdan kale örneği ile siber güvenliğin aynı zamanda nasıl bir anda yerle bir olabileceğine dair de bir gönderme yapmak istiyorum.

Şekil 5. Çok katmanlı güvenliğe örnek olarak kumdan kale[20]

5. Güvenlik Süreci

"*Güvenliğin esası hayatta kalmaktır, ancak aynı zamanda makul bir şekilde varoluş koşullarıyla ilgili önemli bir dizi endişeyi de içerir.*"

Barry Gordon Buzan

Kriptograf ve güvenlik uzmanı *Bruce Schneier*'ın da belirttiği üzere; "*Güvenlik bir ürün değil, bir süreçtir*"[21]. Bu nedenle döngüsel bir şekilde güvenlik analizleri, güvenlik iyileştirmeleri ve güvenlik testleri uygulanmalıdır. Güvenlik süreçleri oyunu okuma ve taktik gerektirir. Savaşın strateji tabanlı olduğu, savaş yapmadan da savaş kazanılabileceği unutulmamalıdır. *Sun Tzu*'nun M.Ö. 6. yüzyılda yazdığı *Savaş Sanatı* isimli kitabında da belirttiği üzere: "*Bir savaşı kazanmak için, kişinin yolu bilmesi gerekir*"[22]. Saldırganın nasıl davranacağına, yapabileceği muhtemel saldırılara dair bir fikre sahip olunması önem arz eder. Gerçek hayatta, karşı saldırı aktif olarak gerçekleşebilse de siber güvenlikte savunma (defensive) temelli bir yaklaşım vardır ve karşı saldırıyı içermez. Ülkelerin siber savaşları bu konuda bir istisnadır.

---

[20] https://upload.wikimedia.org/wikipedia/commons/2/2a/Ultimate_Sand_Castle.jpg, 23.8.2022 tarihinde erişim sağlandı

[21] SCHNEIER Bruce, "The process of security", **Information Security**, 3(4), 32, 2000.

[22] TZU Sun, "Savaş sanatı", **Salon Yayınları**, 2018.

Siber saldırganların ilgisi farklı dönemlerde farklı hedeflere odaklanmakla birlikte; siber güvenlik süreçlerinde her dönem önem verilmesi gereken bazı alanlardan söz etmek mümkündür. *Schneier*'in çalışmasında[23] belirttiği üzere; kritik altyapılar için standartlar geliştirip uygulamaya, siber güvenlik ile ilgili teknolojileri geliştirmek için akademi ve endüstrinin birlikte çalışmasına önem verilmelidir.

Siber güvenlikçilerin sadece temel bilişim güvenliği konusunda bilgi sahibi olmaları da yeterli gelmeyecektir. Bu konuda kendini yetiştirmek isteyen kişilerin; kriminoloji, psikolojik harekât, gayri nizami harp ve terörizm konularında da bilgi sahibi olmasında fayda bulunmaktadır. Güvenlikte stresi iyi yönetmek de önem taşır. Saldırı anında panik yapmamak ve soğukkanlı olmak bir siber güvenlikçinin en önemli meziyetlerinden birisi olmalıdır. Bu konuda siber güvenlikçilere stres eğitimi veren yerler de bulunmaktadır. Örneğin; ülkemizdeki bir girişimde liderlik, ekip yönetimi ve mental dayanıklılık gibi yetenekleri merkeze alan bir eğitim sağlanmaktadır.

Güvenlik süreçlerinde risk analizi aktif bir şekilde kullanılmalıdır. Risk analiz edilerek ilgili riskin oluşma olasılığı ve muhtemel etkisi (*impact*) hesaplanır. Risk değeri, bu iki değerin çarpımı ile hesaplanır. Bu durumda Tablo 1'de gösterildiği üzere, risk; düşük, orta ve yüksek önemli olarak belirlenir. Risk düşükse görmezden gelinebilir. Risk yüksekse alınacak güvenlik önlemleri ile risk kaldırılmaya çalışılır. Bu çoğunlukla mümkün değildir. Bu durumda güvenlik önlemleri alınarak risk azaltılmaya çalışılır. Gerçek hayatta risk başkasına devredilebilir, buna sigorta denir. Günümüzde sigorta firmaları da ticari siber güvenlik sigorta hizmeti sunmaya başlamıştır.

Etki \ Olasılık	Çok olasılık dışı	Olası	Çok olası
Kritik değil	1	2	3
Kayda Değer	2	4	6
İşlemlerin devam etmesi için gerekli	3	6	9

Tablo 1. Risk değerlendirmesi (Yeşil düşük, sarı orta, kırmızı yüksek)

[23] SCHNEIER Bruce, "Memo to Next President: How to Get Cybersecurity Right", **Wired**, 7.8.2008, https://www.wired.com/2008/08/securitymatters-0807/ (Erişim Tarihi: 05.10.2022)

Schneier'in, güvenliğin psikolojisi[24] adlı çalışmasında risk ve korku anlarını algılama süreci sırasında beynin hangi alanlarının kullanıldığının önemi konusu vurgulanmıştır. Tehlike anında ilkel amigdala (*amygdala*) mı yoksa gelişmiş neokorteksimizi mi kullanıyoruz? Bu konudaki tercihimiz duygularımızla panik olup ani karar vermek ile durumu iyice algılayıp karar vermek arasındaki farkı belirlemektedir. Amigdala ile hızlı karar versek de bu her zaman doğru yol olmamaktadır.

Kai, büyük veri anonimleştirmesi hakkında yaptığı sunumunda[25] veri güvenliği/mahremiyeti ve safari aktivitesi arasında bir benzetme yapmaktadır. Ona göre, siber dünyada tıpkı bir safaride gibiyiz ve bu deneyimin keyfini sürüyoruz. Etrafta aslanlar var ve biz araçlarımızın içinde güvende olduğumuzu düşünüyoruz. Zebralar gibi aslanların ilgisini çeken başka hedefler olduğu sürece nispeten güvendeyiz. Evimizde oturup belgesel izlesek aslında hiç risk almayacaktık. Ama siber dünyanın ve verilerimizin nimetlerinden yararlanmak istiyoruz. Örneğin; analiz edilecek verilerde fayda ve güvenlik konusunu ele alırsak, ham veriyi direkt olarak kullandığımızda en fazla fayda alınacaktır fakat aynı zamanda mahremiyet ve güvenlik seviyesi en düşük değerde olacaktır. Riski düşürmek için güvenlik önlemlerini arttırmamız, veriyi işleyerek mahremiyet sıkıntısı oluşturacak kısımları düzenlememiz gerekecektir. Bu işlemler veriden alacağımız faydayı bir miktar azaltsa bile bunu anlamlı bir seviyede gerçekleştirmemizi sağlayacaktır.

Sistemlerin bir çoğunda bulunan zafiyetler, tasarımla güvenlik (*security by design*) ve tasarımla mahremiyetin (*privacy by design*) geliştirme süreçlerine yeterince dâhil edilmemesinden kaynaklanmaktadır. Daha önce de belirttiğimiz gibi, her sisteme saldırılabileceği unutulmamalıdır. Bu nedenle ağ ve sistemler sürekli izlenmelidir. Siber saldırıların hedefleri, kullandıkları yöntemleri ortaya çıkaran siber tehdit istihbaratı bu toplanan verilerin analizi ile mümkün olacaktır. Siber tehdit istihbaratında çeşitli kavramsal modeller kullanılabilir. Örneğin; Acı Piramidi (*Pain Pyramid*) kavramsal modeli, saldırı vektörleri hakkında bilgi sahibi olarak rakiplerin işlerini zorlaştırmaya ve operasyon maliyetlerini arttırmaya vurgu yapmaktadır[26].

---

[24] SCHNEIER Bruce, "The psychology of security", In International conference on cryptology in Africa (pp. 50-79). Springer, Berlin, Heidelberg, 2008.
[25] KAİ XİN Thia, "Lion, zebras and big data anonymization", **Slideshare**, 02.10.2013, https://www.slideshare.net/KaiX/lions-zebras-and-big-data-anonymization (Erişim Tarihi: 05.10.2022)
[26] BİANCO David, "The Pyramid of Pain", **SANS**, 01.07.2014, https://www.sans.org/tools/the-pyramid-of-pain/ (Erişim Tarihi: 05.10.2022)

Saldırılardan sonra da işlemini devam ettirebilen siber esnek (*cyber resilience*) sistemler kurulması hedeflenmelidir. Bilinmeyen bilinmeyenler hakkında eylem planı hazır olmalıdır. Bütün bunlara rağmen, sistemler veya sistemlerdeki veriler ele geçirilebilir. Bu durumlarda neler yapılması gerektiğine dair yönergeler yazılmalı ve gerekli tatbikatlar yapılmalıdır. Kurtarma ve ayaklandırma için eylem planı olmalıdır. Adli bilişim (*forensics*) süreçleri için kullanılacak sitem kayıtlarının düzenli tutulması ve saldırgan tarafından silinmemesi sağlanmalıdır.

6. Ahlak; Suç ve Ceza

Siber güvenlikte ahlak felsefesine sahip olunmalıdır[27]. Örneğin; herhangi bir kurumun sorumlularından izin alınmadan o kuruma ait bir sistemin güvenlik açıkları taranamaz. Siber güvenlik ahlakı (*cyber security ethics*) olarak da nitelendirilen meziyet ise güvenlik konusunda çalışan kişileri, siber saldırganlardan ayıran davranışlar toplamıdır. Diğer bir deyişle, neyin doğru neyin yanlış olduğunun farkında olmak ve ilgili konularda çalışırken ahlaki kurallara uymaktır[28]. Neyin suç olduğunu anlamak için ise Avrupa veri koruma hukuku gibi veri korumaya dair kanunların yeterli olduklarını söylemek henüz mümkün değildir. Halen kullanıcılar verileri üzerinde tam anlamıyla kontrole sahip değildir. Bu tür kanunlar ne yazık ki süreci basitleştirmekten uzaktır[29]. AB Genel Veri Koruma Yönetmeliği (**"GDPR"**) gibi yasalarla bu süreçteki iyileştirme çalışmaları devam etmektedir. Bu tür yasalar sadece Avrupa'yı değil bütün dünyadaki yasa uygulamalarını etkilemektedir[30]. Ülkemizde de kişisel verileri koruma kanunu ("**KVKK**") ile iyileştirmeler sürmekle birlikte kullanıcıların yeterince bilinçli olduğunu söylemek zordur. Saldırganların sanal ortamlarda yapılan ihlallerden dolayı yakalanmayacaklarını, yakalanırlarsa da cezalandırılmayacaklarını düşündükleri birçok olaydan yola çıkarak bunu söylemek mümkündür. Oysa ki her suçun bir cezası vardır. İnternette yaptığımız her harekette iz bırakırız ve siber güvenlik uzmanları bu izleri takip edilerek saldırganları yakalayabilir.

---

[27] JAQUET-CHİFFELLE David-Olivier/LOİ Michele, "Ethical and unethical hacking.", **In The ethics of cybersecurity**, pp. 179-204. Springer, Cham, 2020.
[28] Reciprocity, "The Importance of Ethics in Information Security", 26.2.2021, https://reciprocity.com/the-importance-of-ethics-in-information-security/ (Erişim Tarihi: 05.10.2022)
[29] KOOPS B. J. "The trouble with European data protection law", **International data privacy law**, 4(4), 2014, 250-261.
[30] ALBRECHT Jan Philipp, "How the GDPR will change the world.", **Eur. Data Prot. L. Rev**., 2, 2016, 287.

III. TARTIŞMA ve SONUÇ

Siber güvenlik felsefesini açıklamak için yazılacak her metnin eksik olacağının farkında olarak, kavram üzerinde düşünmenin ve farkındalığının önemini tekrar vurgulamak istiyorum. Ancak böyle bir yaklaşım ile daha güvenilir sistemler kurmamız mümkün olacaktır.

Siber güvenliğin sağlanabilmesi için hukuk boyutunun da teknolojinin gelişimi ile birlikte evrilmesi gerekmektedir. Veri koruma kanunu gibi yasaların günümüz ihtiyacını karşılayabilmesi için hukuk insanları ile teknik ekiplerin birlikte çalışmasının önemini hatırlatmakta fayda vardır. Bu süreçlerde merkezi olmayan (*decentralized*) sistemler ve akıllı sözleşmelerin (*smart contract*) kullanılmasının bir fark yaratabileceğini de belirtmek istiyorum.

Siber güvenlik konusunda bilgili ve donanımlı insan kadrolarına ihtiyacımız bulunmaktadır. Bilgisayar mühendisliği eğitiminde bu konularda ders verilmesinin önemli olduğu kadar hukuk fakültelerinde bu konularda bilinçlendirme çalışmalarının yapılması gereklidir. Kurumlarda bütün çalışanlar siber güvenlik riskleri konusunda bilgilendirilmelidir. Kurum içi siber güvenlik eğitiminde oyunlaştırma yöntemlerinin kullanılması sunulan içeriğin faydasını artıracaktır. Sonuç olarak, kullanıcıları bilinçlendirmeyi sürekli devam eden bütünsel ve dinamik bir süreç olarak ele almamızda fayda bulunmaktadır.

Jonathan Hey'in gelecekte etrafımızdaki bilgileri nefes almamızı hayal etmesi henüz gerçek olmamış olsa bile günümüzde sanal gerçeklik (*virtual reality*) teknolojisi açılımlar vaat etmektedir. Artırılmış gerçeklik (*augmented reality*) ve genişletilmiş gerçeklik (*extended reality*) teknolojileriyle dış dünyaya etkileşimin mümkün olmasıyla dijital dünya ile gerçek dünya arasındaki bağlar kurulmaktadır. Bir siber güvenlik uzmanının sanal gözlüğü ve el ekipmanları ile sistemlerini etkin bir şekilde yönetebilmesi yakında mümkün olabilecektir. Bu aşamalarda yapay zeka ve blokzinciri gibi teknolojilerin etkin kullanımı ile yeni yaklaşımlar söz konusu olacaktır.

Teşekkür
Yazılan bölümü baskı öncesinde okuyarak; düzeltme ve önerileriyle bölüme değer katan Dr. Gözde Ersoy, Hasan Yiğit ve Dr. Ömer Aydın'a teşekkürlerimizle.

Kaynaklar

Akgün, Ali E./KESKİN Halit, "Sosyal bir etkileşim süreci olarak bilgi yönetimi ve bilgi yönetimi süreci." **Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,** 5, no. 1, 2003, 175-188.

ALBRECHT Jan Philipp, "How the GDPR will change the world.", **Eur. Data Prot. L. Rev.**, 2, 2016, 287.

BİANCO David, "The Pyramid of Pain", **SANS**, 01.07.2014, https://www.sans.org/tools/the-pyramid-of-pain/ (Erişim Tarihi: 05.10.2022)

CYCRAFT, "CyCraft Classroom: MITRE ATT&CK vs. Cyber Kill Chain vs. Diamond Model", **Medium**, 01.07.2020, https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f (Erişim Tarihi: 05.10.2022)

GOODE Luke, "Anonymous and the political ethos of hacktivism.", **Popular Communication,** 13, no. 1, 2015, 74-86.

HEY Jonathan, "The data, information, knowledge, wisdom chain: the metaphorical link." **Intergovernmental Oceanographic Commission**, 26, 2004, 1-18.

JAQUET-CHİFFELLE David-Olivier/LOİ Michele, "Ethical and unethical hacking.", In *The ethics of cybersecurity*, pp. 179-204. Springer, Cham, 2020.

KAİ XİN Thia, "Lion, zebras and big data anonymization", **Slideshare**, 02.10.2013, https://www.slideshare.net/KaiX/lions-zebras-and-big-data-anonymization (Erişim Tarihi: 05.10.2022)

KADİVAR Mehdi, "Cyber-attack attributes.", **Technology Innovation Management Review,** 4, no. 11, 2014.

KARAARSLAN Enis, “Web saldırı saptama sistemlerinin etkinleştirilmesi için sistem farkındalığı ve çok katmanlı güvenlik önlemlerinin gerçekleştirilmesi”, Doktora Tezi, **Ege Üniversitesi Fen Bilimleri Enstitüsü**, 2008.

KARAARSLAN Enis/AKBAŞ M. F. “Blokzinciri tabanlı siber güvenlik sistemleri”, **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, *3*(2), 2017, 16-21.

KOOPS B. J. “The trouble with European data protection law”, **International data privacy law**, *4*(4), 2014, 250-261.

LEVY Steven, “*Hackers: Heroes of the computer revolution”*, Vol. 14. Garden City, NY: Anchor Press/Doubleday, 1984.

PAGANİNİ Pierluigi, "The hotel chain Radisson Hotel Group suffered a security breach that exposed personal information of the members of its loyalty scheme.", **Security Affairs**, 31.10.2018, https://securityaffairs.co/wordpress/77530/data-breach/radisson-hotel-group-data-breach.html (Erişim Tarihi: 05.10.2022)

Reciprocity, “The Importance of Ethics in Information Security”, 26.2.2021, https://reciprocity.com/the-importance-of-ethics-in-information-security/ (Erişim Tarihi: 05.10.2022)

SCHNEIER Bruce, “The process of security”, **Information Security**, *3*(4), 32, 2000.

SCHNEIER Bruce, “Memo to Next President: How to Get Cybersecurity Right”, **Wired**, 7.8.2008, https://www.wired.com/2008/08/securitymatters-0807/ (Erişim Tarihi: 05.10.2022)

SCHNEIER Bruce, “The psychology of security”, In *International conference on cryptology in Africa* (pp. 50-79). Springer, Berlin, Heidelberg, 2008.

SHAHJEE Deepesh/WARE Nilesh, "Integrated Network and Security Operation Center: A Systematic Analysis.", **IEEE Access**, 10, 2022, 27881-27898.

STROM Blake E., Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. "Mitre att&ck: Design and philosophy.", In *Technical report*. The MITRE Corporation, 2018.

TZU Sun, "*Savaş sanatı"*, **Salon Yayınları**, 2018.

Yadav, Tarun, and Arvind Mallari Rao. "Technical aspects of cyber kill chain.", In *International symposium on security in computing and communication*, **Springer**, Cham, 2015, 438-452.

WARK McKenzie, "A hacker manifesto [version 4.0]", ***Subsol****, 2004,* *http://subsol.c3.hu/subsol_2/contributors0/warktext.html* (Erişim Tarihi: 05.10.2022)

WARK McKenzie, "Hackers", **Theory, Culture & Society**, *23*(2-3), 2006, 320-322.