thinktech
STM Teknolojik Düşünce Merkezi

Kritik Altyapı ve Stratejik Tesislerin Siber Güvenliği

Güvenlik, tarihin her evresinde insanların öncelikleri arasında bulunmuştur. Her zaman öncelikli olan fiziki güvenlik kavramları ise günümüz teknolojileri nedeniyle siber güvenlik kavramlarıyla yer değiştirmeye devam ediyor. Büyük veri, yapay zekâ, makine öğrenmesi, bulut teknolojisi ve daha birçok yeni teknoloji siber güvenlik endişelerinin artmasında rol oynuyor.

Savunma bir bütün olarak değerlendirildiğinde "siber savunma" bunun önemli bir parçası olarak öne çıkıyor. Örneğin NATO, operasyon alanlarına (kara, hava, deniz) Siber Uzayı ekledi. Son olarak Ukrayna ve Rusya arasında yaşanan savaşın siber dünyaya yansıması veya kritik tesislerin uğradığı siber saldırılar, siber güvenliğin önemini bizlere bir kez daha gösteriyor.

Kritik altyapılar, teknolojik ve dijital sistemlerle desteklenmeye başlayınca bu alanda da ciddi bir siber güvenlik endişesi ortaya çıkıyor. Dünyanın artan enerji ihtiyacıyla gelişen temiz ve yenilenebilir enerji sistemleri, hammadde ve tedarikinde kullanılan yeni nesil sanal paralar ve blockchain teknolojisi, iletişim sistemleri, ulaşım sistemleri, sağlık sistemleri, su dağıtım şebekeleri, teknoloji destekli savunma sistemleri ve daha birçoğu her gün siber saldırılara maruz kalıyor.

Artan siber saldırılar dünya üzerinde uygulanan siber güvenlik uygulamalarının geliştirilerek yeniden değerlendirilmesine neden oluyor. Sağlıklı bir toplum, ticari düzen ve savunma organizasyonu için kritik altyapı ve stratejik tesislerin siber güvenliği büyük önem taşıyor.

Kritik Altyapı Nedir?

Kritik Altyapı, insanların yaşam tarzı için gerekli işlevleri sağlayan varlıklar, sistemler ve ağlar olarak tanımlanıyor. Birbirine bağlı bir ekosistemin parçası olan 16 kritik altyapı sektörü bulunuyor. Bu sektörlere yönelik herhangi bir tehdit, potansiyel olarak ulusal güvenliği, ekonomiyi, kamu sağlığını veya güvenliğini zayıflatabilecek sonuçlara yol açabiliyor[1].

ABD'nin Siber Güvenlik ve Altyapı Güvenlik Ajansı (Cybersecurity and Infrastructure Security Agency -CISA) verilerine göre; kritik altyapı sektörleri kimya sektörü, ticari tesisler, iletişim sektörü, kritik üretim sektörü, barajlar, savunma endüstriyel tesisleri, acil hizmetler sektörü, enerji sektörü, finans hizmetleri sektörü, yiyecek ve tarım sektörü, hükümet tesisleri, kamu sağlığı ve tedavi hizmetleri, bilgi teknolojileri, nükleer reaktör ve materyaller ile nükleer atık sektörü, ulaşım sektörü, temiz ve atık su sektöründen oluşuyor[2].

1 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
2 https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Bütün bu tesis ve sektörlerin siber güvenliği ise kapsamlı ve profesyonel bir yaklaşım gerektiriyor. Her bir sektörün kendi özelinde güvenlik riskleri ve saldırganların hedef alabileceği zayıf yönlerinin belirlenerek buna uygun bir siber güvenlik politikası oluşturulması gerekiyor.

Kritik Altyapılara Yapılan Siber Saldırıların Risk Alanları

Kritik altyapıların kurulması ve devamlılığının sağlanması günümüzde internet altyapısına bağlı olduğundan tüm tehdit kaynakları arasında siber saldırılar son yıllarda belirgin biçimde öne çıkıyor. Bu tehdit türü alınacak önlemlerde yeni ve teknolojiye dayalı birtakım unsurların devreye alınmasına yol açıyor. Her şeyden önce siber saldırılar çok büyük hasarlara yol açabiliyor. Pek çok ülkenin kritik altyapısı ve stratejik tesisleri çeşitli tarihlerde siber saldırıların hedefi olmaya devam ediyor[3].

Kritik altyapılara ve stratejik tesislere yönelik gerçekleştirilen siber saldırıların hedeflediği risk alanları bulunuyor. Bunlar şu şekilde tanımlanıyor:

- **Operasyonel risk**, operasyonların aksama süresini ve şirketin misyonunu yerine getirememesini içeriyor.
- **Güvenlik riski**, çalışanların ve yakındaki diğer kişilerin fiziksel zarar görmesini veya ölmesini içeriyor.

  Çevresel risk, toprağa, su yollarına, hayvanlara, bitki örtüsüne ve insanlara yönelik toksik fiziksel zararları kapsıyor.
- **Yangınlar/patlamalar/ekipman hasarı** tesise ve çevredeki topluluğa fiziksel zarar verebiliyor.
- **Finansal riskler** arasında yasal para cezaları ve diğer cezalar, faaliyet ruhsatı kaybı, hukuki ve cezai davalar, temizleme ve iyileştirme maliyetleri, itibar kaybı ve hisse senedi değer kaybı yer alıyor.
- **Ulusal güvenlik riskleri**, gıda, içme suyu, ısı, yakıt ve elektrik gibi temel uygarlık ihtiyaçlarının kaybına yol açan tedarik zinciri kesintilerinden oluşabiliyor.

Kritik altyapıya uzaktan saldıran bir saldırgan ile bunun sonucunda ortaya çıkabilecek fiziksel etkileri birleştirdiğinizde, ulusal kargaşaya yol açacak bir felaket ortaya çıkabiliyor. Bu nedenle hükümetler kritik altyapı siber güvenliği konusunda giderek daha fazla endişe duyuyor[4].

Kritik Altyapıların Karşılaştıkları Siber Güvenlik Tehditleri

Dünyada ve Türkiye'de kritik altyapıların mevcut durumunu ve temel eğilimlerini anlamak, sözkonusu altyapılara yönelik tehditleri irdelemek ve bunları bertaraf etmek maksadıyla geliştirilen çözüm önerilerini değerlendirmek siber güvenlik stratejilerinde önemli bir yer ediniyor. Birçok ülke kritik altyapılarını korumak ve güvenliğini güçlendirmek için çalışmalar yürütüyor. Ancak her geçen gün değişen teknolojilerin de etkisiyle siber güvenlik konusunda anlık değişimler yaşanabiliyor. Siber güvenlik tehditlerinin günümüz altyapılarına anlık etkilerinin detaylı bir şekilde incelenmesi alınacak önlemlerin verimliğini doğrudan etkiliyor[5].

Birbiriyle bağlantı içinde olan kritik altyapı sistemlerinin artan kullanımı, otomasyon süreçlerinde ve operasyonel verimliliğin artırılmasında önemli avantajlar sunuyor. Ancak bu bağlanabilirliğin olumlu etkisi aynı zamanda önemli siber güvenlik açıklarını da beraberinde getirerek enerji altyapıları, su kaynakları ve sağlık sistemleri gibi kritik kurumları siber saldırılara karşı savunmasız bırakabiliyor.

Kritik verilerin ve sistemlerin fidye yazılımıyla şifrelenmesi yöntemi siber saldırılar içinde hâlen önemli bir yer ediniyor. Bu dosyaların şifresinin çözülmesi için fidye istenebiliyor. Altyapılara veya bütün sistemlere erişimlerin sabote edilmesi veya hassas verileri çalmak için kullanan davetsiz misafirlerin varlığı ile

3 https://thinktech.stm.com.tr/tr/kritik-endustriyel-altyapi-guvenligi-i-enerji-iletim-ve-dagitim-guvenligi
4 https://www.techtarget.com/searchsecurity/tip/Top-6-critical-infrastructure-cyber-risks
5 https://thinktech.stm.com.tr/tr/kritik-endustriyel-altyapi-guvenligi-ii-ulastirma-haberlesme-bilgi-ve-iletisim-teknolojileri-guvenligi

memnuniyetsiz çalışanların sistemlere kasıtlı olarak zarar verme isteği içeriden gelen tehditleri oluşturuyor. DDoS saldırıları ise sistemlerin yanıt verebilirliğini tehlikeye atarak önemli miktarda veri trafiğine neden olup kritik altyapı ve tesislerin kullanılmaz hâle gelmesine neden olabiliyor. Tedarik zinciri saldırıları da bir hedefe ağ erişimi sağlamak amacıyla üçüncü taraf satıcıların ele geçirilmesini içeriyor[6].

Uzaktan çalışma konusu da siber güvenlik tehditlerinin artmasına neden olan bir başka konu olarak öne çıkıyor. Uzaktan çalışanların evlerinde veya çalıştıkları kafe, açık alan vb. tesislerde kullandıkları internet bağlantıları siber saldırganların etkili saldırılar gerçekleştirmesi için bir ortam yaratıyor[7].

Ülke çapında gerçekleşen Advanced Persisten Threat (Gelişmiş Kalıcı Tehdit -APT) gruplarının siber saldırıları da ülkeler için önemli ve büyüyen bir tehdit oluşturuyor. Bu tehditler önemli mali kayıplara neden oluyor ve kritik altyapıyı etkiliyor. APT grup saldırılarından kaynaklanan küresel kayıplar kesin olarak tahmin edilemiyor. Bu durum eksik raporlama ve bu saldırıların genellikle karmaşık ve uzun vadeli doğasından dolayı ortaya çıkıyor.

APT grupları genellikle bir dizi amaç için belirli varlıkları veya sektörleri hedefliyor. Bunlar;

- **Casusluk:** Siyasi, askeri veya endüstriyel avantaj sağlamak için hassas bilgilerin çalınması.
- **Finansal Kazanç:** Veri ihlalleri ve fidye yazılımı saldırıları yoluyla finansal kazanç elde etmek için finansal kurumları ve bireyleri hedeflemek.
- **Sabotaj:** Hasar ve kaosa neden olmak için kritik altyapı ve hizmetleri kesintiye uğratmak.
- **Etkileme Operasyonları:** Kamuoyunu manipüle etmek ve demokratik süreçleri baltalamak için dezenformasyon ve propaganda yaymak olarak değerlendiriliyor.

APT grupları siber güvenlik uzmanlarını atlatabilmek için tekniklerini sürekli olarak güncelleyerek günümüz şartlarına uyarlıyor. Yapay zekâ, otomasyon ve gelişmiş şifreleme operasyonlara giderek daha fazla dahil edilerek, tespit edilmesi ve önlenmesi daha da zorlaşan saldırılar gerçekleştiriliyor[8].

Kritik Altyapı ve Stratejik Tesislerin Siber Güvenliği İçin Atılan Adımlar

Kritik altyapı siber güvenlik tehditleriyle mücadele etmek için devlet kurumlarının tehditlerin niteliğinin yanı sıra güvenlik programlarının ve kontrollerinin performansını da ölçmesi, izlemesi ve anlaması gerekiyor. Tehditler gelişip yayılmaya devam ettikçe, ulusal güvenliği korumakla görevli kuruluşların, güvenlik stratejisi ve politikasını yönlendirebilecek istihbaratı geliştirmenin daha etkili bir yolunu bulması ve kendine uyarlaması gerekiyor[9].

Siber saldırılara karşı alınabilecek bazı genel önlemler bulunuyor. **Tutarlı Risk Değerlendirmeleri** ile güvenlik protokolleri ve güvenlik açıkları sürekli değerlendiriliyor. Çok Faktörlü Kimlik Doğrulama ağ erişimine izin vermeden önce birden fazla kimlik doğrulaması yaparak güvenliği artırıyor. Tüm donanım ve yazılımın sürekli olarak en son sürümlere güncellenmesinin zorunlu hâle getirilmesi savunma araçlarının güncelliğinin korunmasını sağlıyor. Çalışanlara optimum güvenlik protokolleri ve kimlik avı girişimlerini tespit etme becerisi konusunda sürekli eğitim sağlanması gerekiyor. **Olay Müdahale Planı** ise zararı en aza indirmek ve operasyonları gecikmeden geri yüklemek amacıyla çeşitli siber saldırı türlerine karşı dayanıklı bir müdahale stratejisi oluşturmaya yarıyor[6].

6 https://www.cdsec.co.uk/blog/cyber-security-threats-to-critical-infrastructures-how-to-ensure-the-protection-of-vital-facilities
7 https://www.linkedin.com/pulse/what-critical-infrastructure-cyber-security-vulnerabilities/
8 https://www.linkedin.com/pulse/silent-war-unmasking-advanced-persistent-threat-apt-sunil-shilimkar-tvaef/
9 https://www.bitsight.com/glossary/critical-infrastructure-cybersecurity

Siber saldırılara karşı çeşitli teknik çözümleri, yapay zekâ destekli sistemlerle sürekli izleme ve iyileştirmeyi birleştiren kapsamlı bir güvenlik stratejisi içinde uygulamak, APT saldırıları gibi yaygın riskleri azaltmak ve kurumların değerli varlıklarını korumak için oldukça önemli bir konu olarak değerlendiriliyor.

Kurumlar için seçilecek en iyi çözüm; bütçe, güvenlik ihtiyaçları, mevcut altyapı ve teknik uzmanlık gibi çeşitli faktörlere bağlı olarak değişebiliyor. Çözüm yöntemine karar vermeden önce özel gereksinimlerin dikkatlice değerlendirmesi ve farklı seçeneklerin karşılaştırılması önem arz ediyor[8].

Dünyada ve Türkiye'de Kritik Altyapı ve Stratejik Tesislerin Siber Güvenliği

Ülkelerin, siber savunma stratejilerini güçlendirmesi gerekiyor. Bu güçlendirme sadece teknolojik çözümleri içermekle kalmıyor, aynı zamanda eğitim, farkındalık ve uluslararası işbirliğini de kapsıyor. ABD'de kurulan CISA gibi kurumlar, ulusal altyapıların korunması için özel sektörle işbirliği yapıyor ve bilgi paylaşımını teşvik ediyor.

Uluslararası hukuk, kritik altyapılara yönelik siber saldırıları yasaklayan normlar geliştirmeye devam ediyor. Birleşmiş Milletler, siber operasyonlarla ilgili sorumlu devlet davranışı normları üzerinde anlaşmalar yapıyor. Bu normlar, özellikle kritik altyapılara kasıtlı zarar verilmesini veya işleyişinin bozulmasını yasaklayan içeriklerden oluşuyor[10].

NATO'nun 9 Temmuz 2016'daki Varşova Zirvesi sonrası bir siber operasyonlar doktrini oluşturması ve askeri alanda siber yeteneklerin geliştirilmesi bu siber güvenlik endişelerinin aslında çok daha önceden yer edindiğinin bir kanıtı olarak görülüyor. 29 Ocak 2020 tarihinde "NATO Müttefikleri için Siber Uzay Ortak Doktrini" adıyla yayınlanan doktrin, NATO'nun günümüzdeki mevcut siber savunma stratejilerinin temelini oluşturuyor.

Doktrinin yayınlanması sonrası NATO'nun sahip olduğu bilgi teknolojileri altyapısı hızla gelişerek günümüzde kurumun Brüksel'deki siyasi karargâhından aktif olduğu askeri bölgelere kadar 60'tan fazla farklı yeri kapsıyor ve her biriyle entegre çalışıyor[11].

Türkiye'de kritik altyapıların korunması süreci, 1999 yılında AB'ye aday ülke olunmasıyla başladı. Tam üyelik uyum mevzuatı kapsamında çevre başlığı altında yürütülen çalışmalarla kritik altyapıların korunması, teknolojik afetler başlığı altında değerlendiriliyor. Bu kapsamda, teknolojik afetlerin, doğal afetlerin tetiklenmesi sonucunda ya da insan kaynaklı bir kaza, terör veya sabotajdan kaynaklanabileceği ifade ediliyor. Dolayısıyla Türkiye'de kritik altyapıların korunması literatürü güvenlik boyutundan ziyade, afet ve acil durum yönetimiyle özdeşleşiyor.

"Türkiye 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı"na göre kritik altyapılar; "İşlediği verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" olarak tanımlanmaktadır. Ülkemizde "Elektronik Haberleşme", "Enerji" "Finans", "Ulaştırma", "Su Yönetimi" ve "Kritik Kamu Hizmetleri" olarak tanımlanan kritik altyapı sektörlerinin siber tehditler karşısında kamu ve özel sektörün korunmasını sağlayacak tedbirler alınarak ulusal mukavemetin artırılması hedeflenmektedir. Bu çerçevede gerçekleştirilecek çalışmalarda; uluslararası bilgi güvenliği standartlarının kamu ve özel sektörde uygulanmasının yaygınlaştırılması, altyapılarda üretici bağımlılığının önüne geçilmesi, yurtiçinde üretilen verilerin yurtiçinde kalması gibi konular ile bunun yanında, sektörel düzenlemelerin geliştirilmesi ve denetim mekanizmalarının oluşturulması, acil durum hazırlık planlarının hayata geçirilmesi ve güvenli bir teknolojik dönüşümün sağlanması öncelikler arasında yer almaktadır[12].

10 https://igam.org.tr/siber-savasin-yeni-cephesi-kritik-altyapilar/
11 https://bit.ly/3yiwbVg
12 https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf

Türkiye'de yapılan önemli çalışmalardan biri de STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'nin (STM) enerji de dahil olmak üzere kritik altyapıların olası şoklara karşı ne kadar elastik olduğunun değerlendirilebildiği bir karar destek modeli. Geliştirilen modelde siber saldırılar gibi şokların enerji, ulaşım, iletişim gibi farklı altyapılarda yaratacağı nihai etkiler ve olası riskler senaryo tabanlı olarak analiz edilebiliyor. Model; NATO'ya stratejik seviyede karar desteği sunarken, yetkililerin atacakları adımlar ve alabilecekleri önlemler noktasında karar verme süreçlerini kolaylaştırıyor. Bir ülkenin elastikiyeti ile o ülkenin kritik endüstriyel altyapılarının güvenliği arasındaki etkileşimin anlaşılmasına STM, bu modeliyle önemli bir katkı sunuyor. Elastikiyet olgusunun anlaşılması ve değerlendirilmesi bağlamında bütüncül ve kapsamlı bir modele duyulan ihtiyaçtan yola çıkan STM'nin, NATO Müttefik Dönüşüm Komutanlığı için geliştirdiği Elastikiyet Karar Destek Modeli (Resilience Decision Support Model), NATO SHAPE Karargâhında uygulamalı olarak kullanılıyor[3].

NATO Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence - CCDCOE) tarafından Estonya'da düzenlenen, dünyanın en büyük siber savunma tatbikatı Locked Shields-2024'e (Kilit Kalkan-2024) katılan STM'nin siber güvenlik uzmanlarının, Zararlı Yazılım ve Sayısal Teknik Analiz alanlarında başarı göstererek, katılımcıların gerçek bir siber saldırıyı tespit etme ve analiz etme kabiliyetlerine katkı verdiği görülüyor.

Türkiye'yi uluslararası arenada başarıyla temsil eden STM'nin 2023 ve 2024 yıllarında katıldığı Locked Shields tatbikatı, siber savunma kapasitesini artırmanın yanı sıra uluslararası dayanışmayı ve işbirliğini güçlendiren, stratejik karar alma süreçlerini entegre eden ve gerçek zamanlı siber tehditlere karşı koyma yeteneğini geliştiren önemli bir platform olarak öne çıkıyor. Farklı ülkelerden gelen ekipler ortak tehditlere karşı koymak ve siber savunma stratejilerini uluslararası düzeyde uyumlaştırmak için bir araya geliyor[13].

STM, stratejik faaliyet alanı olarak nitelendirdiği siber güvenlikte; entegratör kimliği ile siber tehdit istihbaratından karar destek sistemlerine, uygulamaların güvenliğinden güvenlik seviyelerinin belirlenmesine kadar bütüncül hizmetler sunuyor. Türkiye'nin ilk Siber Füzyon Merkezi olan STM Siber Füzyon Merkezi, 2016'dan beri bu alanda önemli bir rol oynuyor. Milli projelerde görevleri bulunan STM, TSK Siber Savunma Merkezi Projesi ile Emniyet Genel Müdürlüğü Siber Suçlar Daire Başkanlığı Bilgi Güvenliği Projesi'ni başarıyla sürdürmeye devam ediyor. Siber Tehdit İstihbarat Portalı CYTHREAT ve STM BUGSHİELD şirketin öne çıkan siber güvenlik ürünleri arasında yer alıyor.

Kritik altyapılar ulusal ve uluslararası anlamda her zaman büyük önem taşıyor. Bu altyapılara yapılacak siber saldırılar toplumların zarar görmesine, ülkeler için kritik sistem veya hizmetlerin tamamen veya uzun süreli devre dışı kalmasına ve hatta küresel ölçekte krizlere neden olabiliyor. Siber güvenlik uzmanlarının gelişen teknolojiler eşliğinde bilgi ve yöntemlerini sürekli güncellemesi savunma stratejilerinin temelini oluşturuyor.

Özel sektör de dahil birçok paydaşın siber güvenlik konularında ortaklaşa çalışmalar yürütmesi ve siber saldırılara karşı tek bir cephede savunma yapılması mevcut güvenlik sistemlerinin gücünü destekleyebilir. Özellikle savunma sektöründe uygulanan yüksek güvenlik sistemleri ve yöntemleri sivil alanlara da uyarlandığında, hükümetlerin veya kurumların kritik altyapılarının korumasında önemli adımlar atılabiliyor. Bu noktada ülkelerin ve kurumların siber güvenlik risklerinin çok iyi bir şekilde analiz edilerek özelleştirilmiş güvenlik protokolleri oluşturulması faydalı olacaktır. Kritik altyapıların korunması bütün dünyada herkesin yararına olacak önemli bir konu olduğu için bu alanda işbirliği hâlinde hareket edilmesi büyük önem taşıyor.

13 https://www.stm.com.tr/tr/medya/haberler/stmnin-siber-guvenlik-uzmanlari-nato-tatbikatinda-yeteneklerini-sergiledi