thinktech
STM Teknolojik Düşünce Merkezi

Dijital Bağışıklık Sistemleri

Dijitalleşme, hayatın her alanında gelişmenin, inovasyonun ve sürdürülebilirliğin anahtarı hâline geldi. Ancak dijital sistemler gelişmeye devam ettikçe siber saldırıların da giderek daha fazla hedefi olmaya başladı. Zira gelişen teknolojiler, siber saldırıların da çeşitlenip artmasına yol açmaktadır. Ayrıca yazılımlar geliştirilirken doğal olarak sahip oldukları kusurlar (bugs) da artmaktadır. Tüm bu zafiyetler kuruluşların dijital sistemlerinin zaman zaman çökmesine, saldırganların eline geçmesine, dolayısıyla büyük maddi kayıplara ve güvenlik problemlerine yol açıyor.

Teknoloji dünyası siber saldırılarla mücadele etmek için geliştirdiği çeşitli yöntemlerin arasına son dönemlerde "Dijital Bağışıklık Sistemleri (Digital Immune Systems)" adı verilen bir unsuru da dahil etmek üzere harekete geçti. Doğadan, hatta doğrudan insan vücudunun çalışma prensiplerinden ilham alan bir sistem olan dijital bağışıklık sistemleri ile uzmanlar, kuruluşların siber bağışıklık kazanması için çalışmalar yürütüyor.

Günümüz siber güvenlik sistemleri, siber saldırılara karşı etkili bir savunma mekanizması sağlamakla birlikte, geleneksel güvenlik duvarı ve izinsiz giriş tespit sistemleri gibi tedbirler şimdiye kadar bilinmeyen saldırıları tespit edip püskürtmekte genellikle zorlanmaktadır. Bir siber bağışıklık sistemi ise yeni, bilinmeyen siber saldırıları tespit edip güçlü bir savunma mekanizması sağlayarak bu eksikliği azaltabilmektedir.

Dijital Bağışıklık Sistemi Nedir?

Teknoloji danışmanlık firması Gartner'in "2023'ün ilk 10 stratejik trendi" listesinde önerdiği Dijital Bağışıklık Sistemi; üstün kullanıcı deneyimi (User Experience -UX) oluşturmak ve iş performansını etkileyen sistem arızalarını azaltmak için yazılım tasarımı, geliştirme, otomasyon, operasyonlar ve analitik kapsamında çeşitli uygulama ve teknolojileri entegre eden bir sistemi ifade etmektedir. Güçlü bir dijital bağışıklık sistemi sayesinde, uygulama ve hizmetler, yazılım hatalarının etkileri veya güvenlik sorunları gibi anormalliklere karşı daha dayanıklı hâle getirilerek korunmakta ve uygulamaların arızalardan hızla kurtulmaları sağlanabilmektedir. Böylece kritik uygulamalar ve hizmetler ciddi şekilde tehlikeye girdiğinde veya tamamen çalışmayı durdurduğunda ortaya çıkan iş sürekliliği riskleri azaltılabilmektedir[1].

1 https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter

İnsan Bağışıklık Sisteminden Dijital Bağışıklığa

İnsanların hastalıklardan korunmak için bağışıklık sistemlerini sağlıklı tutmaya çalışmaları gibi siber güvenlik ekosistemi de dijital tehditlere karşı koymak için güçlü bir siber bağışıklık sistemine ihtiyaç duymaktadır[2]. Biyo-ilhamlı bilgi işlem olarak da adlandırılan bu süreç, çeşitli araştırma alanlarında doğanın esin kaynağı olarak görülmesinden hareket etmektedir. Yeni bir araştırma alanı olan siber bağışıklık sistemleri, yeni, görünmeyen patojenleri tespit etme ve savuşturma kabiliyeti nedeniyle insan ve hayvanların adaptif bağışıklık sistemini taklit etmeye çalışır[3].

Biyo-ilhamlı bilgi işlem, bilgisayarları doğayı modellemek için kullanmakta ve aynı anda bilgisayar kullanımını geliştirmek için doğayı incelemektedir. Biyo-ilhamlı bilgi işlem, evrimsel süreçlere dayalı genetik algoritmalar, Yapay Zekâ ve Yapay Sinir Ağları, sensör ağları (duyu organları) veya yapay bağışıklık sistemlerini içerir. Siber bağışıklık sistemleri genellikle yapay zekânın bir alanı olan Makine Öğrenmesi yöntemlerini kullanır. Makine öğrenmesi, bilgisayarlarda insan öğrenme yeteneklerini taklit ettiği için biyo-ilhamlıdır denebilir.

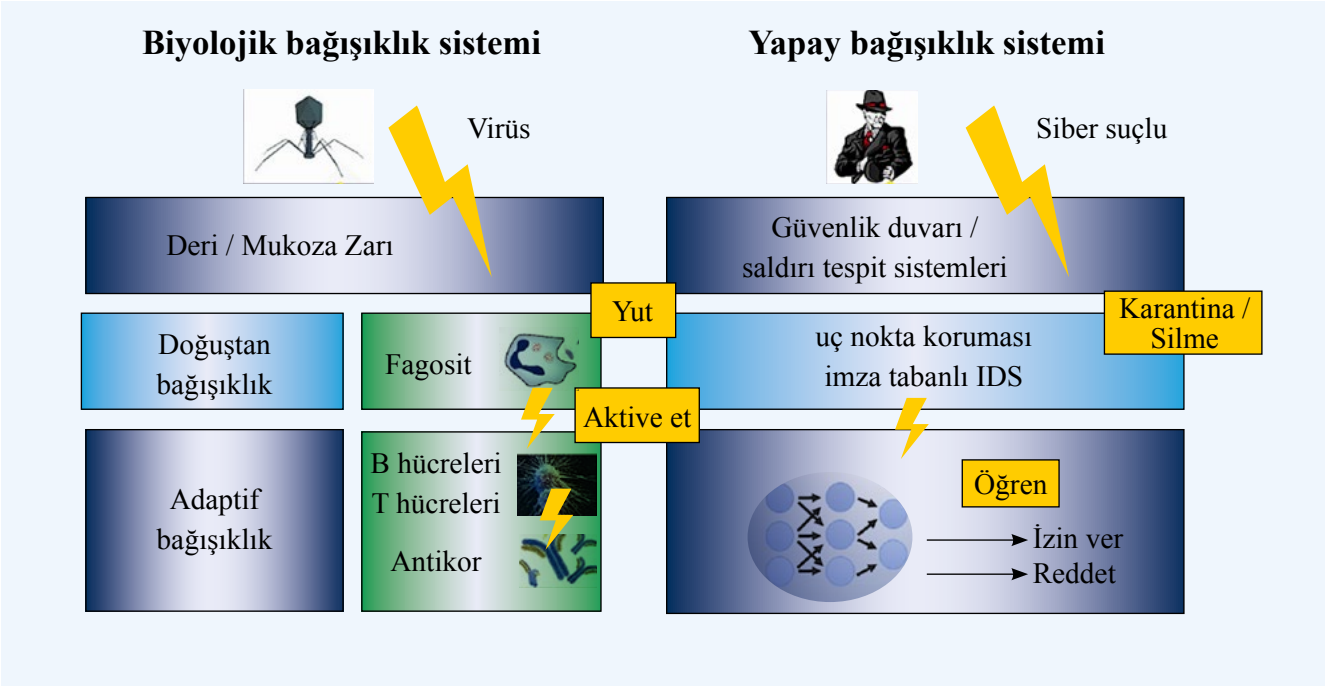
Dijital bağışıklık ya da siber bağışıklık yaklaşımının felsefesini kavramak için bir metafor olarak insan vücudunun bağışıklık sistemi ve mekanizması kullanılmaktadır. İnsan vücudu, virüsler, parazitler ve mikroplar gibi patojen adı verilen çok çeşitli zararlı ajanları tespit eden, oldukça etkili bir savunma mekanizmasına -bağışıklık sistemine- sahiptir. Bağışıklık sistemi, patojenleri sağlıklı dokudan ayırt etme yeteneğine sahiptir. Cilt, bir güvenlik duvarına benzer şekilde vücudumuza yönelik dış tehditleri savuşturmakta, sürekli yenilenip uyarlanmaktadır. Bağışıklık sisteminin etkin çalışmaması durumunda en küçük enfeksiyonlar bile ölümcül hâle gelebilmektedir.

Bağışıklık sistemi, doğuştan gelen bir bağışıklık sisteminden ve bir adaptif bağışıklık sisteminden oluşur. Bir patojen doğuştan gelen bağışıklık sisteminden kaçarsa, adaptif bağışıklık sistemi etkinleştirilir. Adaptif bağışıklık sistemi patojene özgü, uyarlanmış bir yanıt üretebilir. Antijene özgüdür ve aynı patojenin vücuda ikinci kez girmesi durumunda yanıt hatırlanır. Bağışıklık sistemi öğrenme, hafıza ve örüntü tanıma yeteneğine sahiptir.

Adaptif bağışıklık sistemi lenfositlerden oluşur. Ana tipler B ve T hücreleridir. B hücreleri, yüzeylerindeki antikorlar belirli bir yabancı antijene bağlandığında patojenleri tanımlar. Vücuda bir antijen girmesi durumunda, bağışıklık sistemi, öldürücü T hücreleri adı verilen özelleşmiş bağışıklık hücrelerini enfeksiyon bölgesine çeken sinyal moleküllerini aktive eder. Öldürücü T hücreleri, virüsler ve diğer patojenler tarafından enfekte olmuş hücreleri veya diğer işlevsiz hücreleri yok eder. B ve T hücreleri aktive edildiğinde çoğalmaya başlar ve yavrularından bazıları uzun ömürlü hafıza hücreleri hâline gelir. Bir siber bağışıklık sistemi bu davranışı taklit eder. Uyarlanabilir ve hafıza işlevselliğine sahiptir ve örüntü tanımayı kullanarak siber tehditleri tanır[3].

Klasik güvenlik duvarları, saldırı tespit sistemleri veya uç nokta koruması gibi geleneksel siber güvenlik sistemleri, yeni, bilinmeyen güvenlik açıklarından yararlandıkları için sıfırıncı gün saldırılarını veya Gelişmiş Kalıcı Tehditleri tespit edemediklerinden koruma sağlamada artık yeterli olamamaktadır. Günümüzün siber güvenlik ihtiyaçlarını karşılamak için bir siber savunma sisteminin, bilinmeyen saldırıları tanıma ve püskürtme ve işi kesintiye uğratmadan yeni tehditlere uyum sağlama yeteneğine ihtiyacı vardır. Tüm güvenlik açıklarının bilinmesinin bir yolu olmadığı için, saldırı modellerini öğrenmek için kullanılabilecek tek kaynak, siber saldırılarla ilişkilendirilen olay dizileridir. Siber bağışıklık, bilinmeyen imzalara sahip saldırıları öğrenip tespit edebilen, biyolojik olarak insan adaptif bağışıklık sisteminden ilham alan bir yaklaşımdır (Şekil 1). Ayrıca siber bağışıklık normal ağ davranışını öğrenir, öğrendiklerine dayanarak anormallikleri tespit eder ve makine öğrenmesi tekniklerini kullanarak adaptif bağışıklık sistemini taklit eder.

2 https://www.avanade.com/en/blogs/avanade-insights/security/immune-system-against-cybersecurity-threats
3 https://www.researchgate.net/publication/315861769_Cyber_Immunity_-_A_Bio-Inspired_Cyber_Defense_System



Şekil 1: Biyolojik ve yapay bağışıklık sisteminin karşılaştırılması[3].

Siber Bağışıklık Sistemlerinin Çalışma Biçimi

Siber bağışıklık sistemleri, saldırıları imzalarına göre değil, normal ağ trafiğinde tespit edilen anormalliklere göre tespit etmektedir. Şimdiye kadar bilinmeyen saldırıları algılamak ve hatırlamak için öğrenme ve hafıza yetenekleri vardır ve siber güvenlik sistemleri ailesine aittirler. Siber güvenlik, bilgisayarları, ağları, programları ve verileri saldırı, yetkisiz erişim, değişiklik veya imhadan korumak için tasarlanmış teknolojiler ve süreçler kümesidir. Siber bağışıklık sistemleri genellikle makine öğrenmesi tekniklerini benimsediklerinden kuralları kendilerinin öğrenebilmesi avantajına sahiptirler. Ayrıca, şimdiye kadar bilinmeyen yeni anormalliklerin meydana gelmesi durumunda, çalışma sırasında yeni kurallar öğrenebilirler.

İnsan vücuduna giren bir virüsün DNA'sı değişir, bu nedenle bağışıklık sistemi virüsün imzasını tanımak için uyum sağlamak zorundadır. Benzer şekilde siber güvenlikte de sürekli gelişen bir düşmanla uğraşılmak zorundadır. Saldırı bilinmediği için öncekilerden saldırının imzası öğrenilemez. Bir siber bağışıklık sistemi, saldırı imzalarını öğrenmek yerine, normal ağ trafiğinin uzun bir süre boyunca nasıl göründüğünü öğrenir. Eğitildikten sonra, belirli bir sapkın modelin kötü niyetli olma olasılığını hesaplar. Sonuçlarını yeni kanıtlara dayalı olarak sürekli günceller. Saldıran bir ajanı gözlemleyerek ve ajanın hangi bilgilerin peşinde olduğunu ve nereden geldiğini tespit ederek önünü kesebilir[3].

Dijital Bağışıklık Sistemlerine Neden İhtiyaç Var?

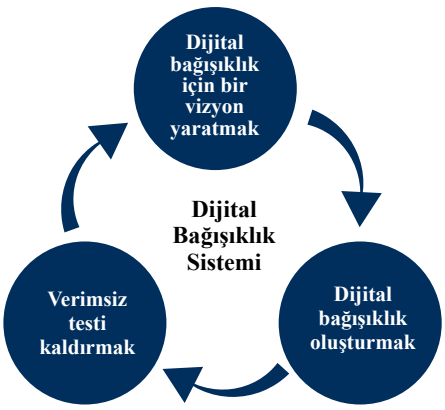
Yazılım uygulamalarına yönelik olarak ortaya çıkan güvenlik açıklarının ve tehditlerin sayısı gün geçtikçe artmaktadır. Siber saldırı ve virüs tehditlerine karşı umut verici olarak görülen yaklaşımların zaman içinde etkisini kaybetmesi, yazılım mühendisliği liderlerinin stratejilerini gözden geçirmelerini sağladı. Yazılımcılar artık yazılım kalitesine yönelik yaklaşımlarının ötesine geçerek dijital bağışıklık sistemlerini benimsemeye yönelmektedir[3].

Güçlü Bir Dijital Bağışıklık Sistemi Oluşturmak İçin Yapılması Gerekenler

Gartner, güçlü bir dijital bağışıklık oluşturmak için, yazılım ekiplerinin aşağıdaki koşulları içeren altı önemli uygulama ve teknolojiyi benimsemesini önermektedir[1]:

- **Gözlemlenebilirlik,** yazılım ve sistemlerin "görülebilmesini" sağlar. Uygulamalara gözlemlenebilirlik eklemek, güvenilirlik ve esneklikle ilgili sorunları azaltmak ve kullanıcı davranışını gözlemleyerek kullanıcı deneyimini iyileştirmek için gerekli bilgileri sağlar.
- **Yapay zekâ ile artırılmış test,** kuruluşların yazılım testi faaliyetlerini insan müdahalesinden giderek daha bağımsız hâle getirmelerini sağlar. Geleneksel test otomasyonunu tamamlar, genişletir ve tam otomatik planlama, bakım ve test analizini içerir.
- **Kaos mühendisliği,** karmaşık bir sistemdeki güvenlik açıklarını ve zayıflıkları ortaya çıkarmak için deneysel testler kullanır.
- **Otomatik düzeltme,** işlevlerini doğrudan bir uygulamada oluşturmaya odaklanır. Kendini izler ve sorunları algıladığında otomatik olarak düzeltir ve operasyon personelinin müdahalesine gerek kalmadan normal çalışma durumuna döner. Ayrıca, başarısız bir kullanıcı deneyimini düzeltmek için gözlemlenebilirliği kaos mühendisliği ile birlikte kullanarak sorunları önleyebilir.
- **Site güvenilirlik mühendisliği,** kullanıcı deneyimini ve elde tutmayı iyileştirmeye odaklanan bir dizi mühendislik ilkesi ve uygulamasıdır. Hız ihtiyacını istikrar ve riske karşı dengeler ve geliştirme ekiplerinin iyileştirme ve teknoloji (görev ihlali/kusuru) konusundaki çabalarını azaltır.
- **Yazılım tedarik zinciri güvenliği,** yazılım tedarik zinciri saldırıları riskini ele alır. Yazılım malzeme listeleri, yazılım tedarik zincirlerindeki tescilli ve açık kaynak kodunun görünürlüğünü, şeffaflığını, güvenliğini ve bütünlüğünü geliştirir. Güçlü sürüm kontrol politikaları, güvenilir içerik için yapı havuzlarının kullanımı ve teslimat yaşam döngüsü boyunca satıcı riskinin yönetimi, dahili ve harici kodun bütünlüğünü korur.

Dijital bağışıklık sisteminin uygulanmasındaki temel unsurlar, büyük ölçüde yazılım mühendisliği liderlerinin vizyon oluşturma, dijital bağışıklık oluşturma ve verimsiz testleri ortadan kaldırma rolüne dayanır.



Şekil 2: Dijital Bağışıklık Sistemi.

Dijital Bağışıklık Sisteminin Önemi

Dijital bağışıklık sistemi, yazılım şirketlerinin hataya karşı daha dayanıklı ve daha yüksek esnekliğe sahip bir yazılım uygulaması oluşturmasına yardımcı olur. Dijital bağışıklık sistemindeki teknolojilerin ve uygulamaların birleşimi, yazılım mühendisliği ekiplerinin işlevsel hatalar, güvenlik açıkları ve veri tutarsızlıkları dahil olmak üzere tehditleri ve güvenlik açıklarını ele almada görünürlük kazanmasını sağlar[4].

Özünde dijital bağışıklık sistemi, çeşitli yazılım mühendisliği stratejileri, tasarım, geliştirme, teknolojiler, veri analitiği, otomasyon ve operasyon kombinasyonları aracılığıyla yazılım uygulamalarının geliştirilmesinde daha iyi güvenlik ve risk yönetimi kurarak uygulamaları ve hizmetleri korumayı amaçlar. Dijital bağışıklık sisteminden

4 https://www.e-spincorp.com/what-is-digital-immune-system-and-its-importance/

gelen uygulama ve yaklaşımlar, uygulamanın esnekliğini artırmaya yardımcı olur, böylece anormalliklerin sürekli tespiti gibi risklere karşı otonom hafifletme ve proaktif eylem yoluyla sistem arızalarını azaltır ve operasyonlara yönelik veri odaklı içgörülerden yararlanır[5].

Güçlü Bir Siber Bağışıklık Sisteminin Özellikleri

İnsan bağışıklık sisteminin birçok yönden sağlıklı oluşmasına benzer şekilde, siber bağışıklık sisteminin gücü de aşağıdaki yedi özelliğe sahip olmasına bağlıdır[2]:

- Kimlik, uygulama, altyapı, veri ve ağ dahil olmak üzere tüm güvenlik alanlarına uygulanan güvenli ve katmanlı erişim ile **sıfır güven mimarisini** benimsemek.
- Veri kaybını önlemek, güvenli e-postaları sağlamak, mobil ve web güvenliğini bireyin ilk savunma hattı olarak yerleştirmek için **veri ve bilgi koruma çözümleri kurmak.**
- Kuruluş tarafından kullanılan tüm işyeri ve dijital platformlar için **uç nokta tespitini ve korumasını güvence altına almak.**
- Uygulama tasarımı ve geliştirmenin erken aşamasında güvenlik açıklarını ortadan kaldırarak **uygulamaların güvenliğini sağlamak.**
- Anonim etki alanlarının kapsamlı bir ağ güvenliği taraması, IP adreslerinin filtrelenmesi, proxy tespiti ve daha güçlü izinsiz giriş koruması çözümleri ile **çevre kontrollerinin güvenliğini sağlamak.**
- Kimlik avı, web tehditleri, sık parola değişiklikleri ve son kullanıcı eğitim oturumları hakkında şirket çapında eğitim yoluyla **bir siber kültür oluşturmak** ve şirket içi işgücü güvenlik politikaları ve bilgi teknolojileri standartları hakkında **farkındalık yaratmak**.
- Tehditleri erken kuluçka döngüsünde ortadan kaldırmak için tüm kritik kontrol kaynaklarından toplanan analizlerin eksiksiz bir izleme görünümünü sağlayan **daha güçlü bir güvenlik zekâsı panosu oluşturmak**.

Dijital Bağışıklık Sistemleri Henüz Emekleme Aşamasında

Siber saldırılar, günümüzün bilgisayar sistemleri için sürekli bir tehdit oluşturmakta ve saldırıların sayısı her yıl artmaktadır. Bu durum, yeni, daha önce karşılaşılmamış saldırı modellerine hızla tepki verebilen siber güvenlik sistemleri için bir talep yaratmaktadır. Bir siber bağışıklık sistemi, bilinmeyen yeni tehditleri algılayabilir ve bunlara uyum sağlayabilir. Ancak klasik siber savunma sistemlerine bir ek olduğuna; geleneksel güvenlik duvarı, saldırı tespit veya uç nokta koruma çözümlerinin yerine geçmediğine dikkat etmek gerekir. Örneğin, siber bağışıklık sistemleri imzası bilinmeyen saldırıları tespit edebilirken, yönetici haklarının izinsiz kullanımını normal bir davranış olarak kabul ettiğinden tespit edememektedir.

Operasyonlar sırasında görünmeyen saldırı modellerini öğrendikleri için, genellikle yeni, öğrenilmiş anormallikleri diğer siber bağışıklık sistemleriyle paylaşırlar. Dağıtık tehdit veritabanlarını kullanarak "kitlenin bilgeliğinden" yararlanırlar ve bunları yeni tespit edilen güvenlik açıklarıyla güncellerler. Dağıtık doğası ve yüksek kullanılabilirlik gereksinimi nedeniyle bulut çözümleri, dağıtık siber bağışıklık çözümleri için iyi bir seçim olarak kabul edilmektedir. Öğrenme yeteneklerine sahip bulut tabanlı siber bağışıklık çözümlerinin erken uygulamaları zaten mevcut olmakla birlikte, hâlâ yüksek yanlış pozitif oranlarına eğilimlidirler ve birçok durumda hâlâ insan muhakemesi gerekmektedir. Bununla birlikte, bilişsel teknolojilerin yakında siber suçluları önemli ölçüde yavaşlatacak kadar olgunlaşması ve mevcut bir güvenlik "suçunun" bir saldırıyla ilişkilendirilip ilişkilendirilemeyeceğine bakılmaksızın doğruluğun yakın gelecekte artması beklenmektedir. Piyasada hâlihazırda siber bağışıklık sistemleri bulunsa ve patentler alınmış olsa da siber bağışıklık alanı henüz emekleme aşamasındadır ve özellikle tipik olarak yüksek sayıda yanlış pozitiften kaçınmak için daha fazla araştırmaya ihtiyaç bulunduğu düşünülmektedir[3].

5 https://www.e-spincorp.com/why-does-digital-immune-system-matter-in-enhancing-cx/