

BİR TIBBİ CİHAZ HACKLENEBİLİR Mİ?

TS EN IEC 81001-5-1 Standardı ve Tıbbi Cihazlarda Siber Güvenliğin Yeni Anlamı

Barış ÇORUH -Biyomedikal Yüksek Mühendisi
bariscoruh@gmail.com

Bir tıbbi cihazın güvenli olup olmadığını düşündüğümüzde aklımıza genellikle benzer sorular gelir: Doğru ölçüyor mu? Doğru doz veriyor mu? Yazılım beklediğimiz gibi çalışıyor mu? Elektriksel olarak güvenli mi? Fakat bağlantılı sağlık teknolojilerinin yaygınlaşması bu listeye yeni ve oldukça farklı bir soru ekledi: **Cihaza başka biri müdahale edebilir mi?**

Bugünün hasta başı monitörleri, infüzyon pompaları, görüntüleme sistemleri, giyilebilir cihazları ve yazılım tabanlı tıbbi cihazları artık yalnızca klinik fonksiyonlarını yerine getiren bağımsız ürünler değil. Hastane ağlarına, bulut sistemlerine, mobil uygulamalara ve uzaktan izleme platformlarına bağlanan dijital sistemlerin parçaları. Bu bağlantılar sağlık hizmetini daha erişilebilir ve verimli hale getirirken yeni bir risk alanı da yaratıyor: **siber güvenlik artık yalnızca bilgi güvenliği değil, aynı zamanda hasta güvenliği meselesi.**

Tıbbi Cihazlarda Siber Güvenlik Problemi Artık Teorik Bir Risk Değil

Tıbbi cihazlarda siber güvenlik probleminin bugün ne duruma geldiğini görmek için çok uzağa gitmeye gerek yoktur. Ocak 2025'te ABD Gıda ve İlaç Dairesi (FDA), iki hasta başı monitörü modeli hakkında bir siber güvenlik uyarısı yayımladı. Tespit edilen zafiyetler, yetkisiz kişilerin cihazı uzaktan kontrol edebilmesine veya cihazın amaçlandığı şekilde çalışmasını engelleyebilmesine olanak verebilecek nitelikteydi. FDA ayrıca cihaz yazılımında bir "arka kapı" (backdoor) bulunduğunu ve internete bağlanan cihazların hasta verilerini sağlık kuruluşunun ortamı dışına aktarabildiğini bildirdi. FDA o tarihte bu zafiyetlerle ilişkilendirilmiş bir yaralanma veya ölümden haberdar olmadığını da özellikle belirtti. Temmuz 2025'te yayımlanan güncellemede ise üreticinin çözümü dikkat çekiciydi: ilgili yazılım yaması cihazların ağ bağlantısı işlevini tamamen kaldı-

ıyordu. Bu örnek, modern tıbbi cihaz dünyasındaki değişimi oldukça iyi göstermektedir.

Bir cihazın sensörü doğru çalışabilir. Elektronik tasarımı güvenli olabilir. Yazılımı bütün fonksiyonel testlerden geçmiş olabilir. Ama bütün bunlar artık tek başına yeterli değildir. **Çünkü cihazın dış dünyayla kurduğu bağlantı, ürünün güvenlik sınırlarının bir parçası haline gelmiştir (Şekil 1)**



Şekil 1 – Tıbbi Cihazın Değişen Güvenlik Sınırı

Siber Güvenlik Neden Hasta Güvenliğinin Parçası Oldu?

Sağlık sektöründeki siber saldırıların etkisi yalnızca tıbbi cihazlarla sınırlı değildir. 21 Şubat 2024'te başlayan Change Healthcare siber saldırısı, bunun ölçeğini gösteren önemli örneklerden biri olmuştur. ABD'nin sağlık teknolojisi ve reçete/ödeme işleme altyapısının önemli aktörlerinden birini hedef alan bu fidye yazılımı saldırısı, sağlık hizmetlerinin dijital altyapıya ne ölçüde bağımlı hale geldiğini görünür kılmıştır. ABD Sağlık ve İnsan Hizmetleri Bakanlığı (HHS), olayın sağlık hizmetleri ve ödeme sistemleri üzerindeki etkisini "benzeri görülmemiş" ölçekte değerlendirmiş ve Temmuz 2025 itibarıyla olaydan yaklaşık 192,7 milyon kişinin etkilendiği bildirilmiştir. Buradaki önemli nokta yalnızca veri ihlali değildir. Bir sağlık sisteminin dijital altyapısının kullanılamaz hale gelmesi; hasta kabulünden reçeteye, laboratuvar sonuçlarından görüntülemeye, ödeme sistemlerinden klinik karar süreçlerine kadar

gerçek sağlık hizmetlerini etkileyebilir. HHS de güncel siber güvenlik kaynaklarında sağlık kuruluşlarına yönelik saldırıların hasta bakımı ve operasyonel sürekliliğin hemen her alanını etkileyebildiğini vurguluyor.

Yukarıda bahsedilen olay yalnızca ABD'ye özgü değildir. Avrupa Birliği de sağlık sektörünü kritik siber güvenlik alanlarından biri olarak ele almaktadır. NIS2 (Ağ ve Bilgi Güvenliği) Direktifi (EU 2022/2555), sağlık dâhil yüksek kritikliğe sahip sektörlerdeki belirli kuruluşlar için siber risk yönetimi ve önemli olayların bildirilmesine ilişkin yükümlülükleri güçlendirmektedir. Avrupa Komisyonu ayrıca 2025'te hastaneler ve sağlık hizmeti sunucularının siber güvenliğini güçlendirmeye yönelik özel bir Avrupa Eylem Planı açıklamıştır. Plan; önleme, tehdit tespiti, müdahale ve toparlanma başlıklarını birlikte ele almaktadır.

2025-2026 döneminde planlanan ve kademeli olarak hayata geçirilen çalışmalar arasında sağlık sektörüne özgü siber olgunluk değerlendirmeleri, tıbbi cihazlar ve elektronik sağlık kayıtları için bilinen ve aktif olarak istismar edilen zafiyetlerin izlenmesi, eğitim çalışmaları ile AB çapında erken uyarı ve fidye yazılımı sonrası toparlanma hizmetleri bulunmaktadır. Böylece siber güvenlik, yalnızca tek bir cihazın korunması değil, sağlık hizmetinin sürekliliğinin korunması problemi haline gelmektedir.

Bu sorun hâlâ ortadan kalkmış değildir. HHS, Nisan 2026'da dört ayrı fidye yazılımı soruşturmasına ilişkin uzlaşma duyururken bu olayların toplamda 427 binden fazla kişiyi etkilediğini açıklamış ve siber saldırıların ve fidye yazılımının kuruma bildirilen büyük ölçekli veri ihlallerinin en sık görülen türü olduğunu belirtmiştir. Dolayısıyla sağlık teknolojilerinde artık üç kavram birbirinden tamamen bağımsız düşünülmemektedir:

- **Emniyet:** Cihazın hastaya, kullanıcıya veya çevreye kabul edilemez fiziksel ya da klinik zarar oluşturmaması,
- **Etkililik:** Cihazın amaçlanan klinik veya sağlıkla ilgili işlevini beklenen şekilde yerine getirmesi,
- **Siber Güvenlik:** Sistemin yetkisiz erişim, manipülasyon, veri ihlali ve diğer siber tehditlere karşı korunması.

Bir cihaz güvenli olabilir ama siber açıdan savunmasızsa güvenli kalacağı garanti edilemez. Tam da bu noktada TS EN IEC 81001-5-1 standardı (Sağlık yazılımı ve sağlık BT sistemleri emniyeti, etkinliği ve güvenliği - Bölüm 5-1: Güvenlik - Ürün yaşam döngüsündeki faaliyetler) devreye girmektedir.

TS EN IEC 81001-5-1 Standardı Ne Söylüyor?

TS EN IEC 81001-5-1:2021 standardı, sağlık yazılımları ve sağlık bilgi teknolojisi sistemlerinde güvenliği ürün yaşam döngüsünün bir parçası haline getiren uluslararası bir standarttır. Standartın yaklaşımını tek cümlede özetlemek mümkün: **Siber güvenlik ürüne sonradan eklenen bir özellik değil, ürünle birlikte tasarlanması gereken bir yaşam döngüsü faaliyetidir.**

Uluslararası Elektroteknik Komisyonu (IEC), standardın amacını sağlık yazılımının siber güvenliğini artıracak faaliyet ve görevleri yaşam döngüsü süreçlerine yerleştirmek ve yazılım yaşam döngüsü süreçlerinin kendisini daha güvenli hale getirmek olarak tanımlamaktadır. Standart aynı zamanda TS EN IEC 62443-4-1 (Endüstriyel otomasyon ve kontrol sistemleri için güvenlik - Bölüm 4-1: Güvenli mamul geliştirme ömür çevrimi gereklilikleri) standardındaki güvenli ürün geliştirme yaklaşımını sağlık yazılımının özel ihtiyaçlarına uyarlamaktadır. Bu küçük gibi görünen değişiklik aslında ürün geliştirme felsefesinde önemli bir dönüşüm yaratmaktadır. Eski yaklaşımda geliştirme sürecinin sonunda bir penetrasyon testi yapmak ve bulunan açıkları kapatmak yeterli görülebilirken, TS EN IEC 81001-5-1 standardı kapsamında ise soru çok daha erken sorulmaktadır: **"Bu sistem daha mimari tasarım aşamasında nasıl saldırıya uğrayabilir?"**

Güvenli Yazılım Nasıl Geliştirilir?

Bir tıbbi cihazın yazılımını geliştirdiğimizi düşünelim. Önce sistemin korunması gereken varlıklarını belirliyoruz. Hasta verileri, cihaz konfigürasyonu, tedavi parametreleri, kullanıcı kimlikleri veya yazılım güncelleme mekanizması bunlardan bazıları olabilir. Sonra soruyoruz: **Bu varlıklara kim, nasıl saldırabilir?** Buradan tehditler ve olası zafiyetler ortaya çıkıyor. Ardından güvenlik gereksinimleri geliştiriliyor: kimlik doğrulama, erişim kontrolü, şifreleme, güvenli haberleşme, kayıt tutma veya yazılım bütünlüğünün korunması gibi. Ancak süreç burada bitmiyor. Bu gereksinimlerin mimariye aktarılması, uygulanması, test edilmesi ve kanıtlarının saklanması gerekiyor.



Şekil 2 – Siber Güvenlik Kanıt Zinciri

Şekil 2’de gösterilen zincirin önemli özelliği şudur: Her güvenlik kontrolünün **neden var olduğunu** ve gerçekten **çalıştığının nasıl kanıtlandığını** gösterebilmeliyiz. Bu nedenle TS EN IEC 81001-5-1 standardı yalnızca siber güvenlik ekiplerinin ilgilendiği teknik bir standart değildir. **Yazılım geliştirme, risk yönetimi, kalite yönetimi, tasarım kontrolü ve ürün sonrası gözetim süreçlerinin tamamına dokunmaktadır.**

Ürün Piyasaya Çıktığında Güvenlik Bitmiyor

Tıbbi cihazlarla diğer birçok mühendislik ürünü arasındaki önemli farklardan biri uzun kullanım ömürleridir. Bir tıbbi cihaz yıllarca klinik ortamda kalabilir. Fakat cihazın piyasaya çıktığı gün bilinmeyen bir güvenlik açığı birkaç yıl sonra keşfedilebilir. Kullanılan üçüncü taraf bir yazılım kütüphanesinde yeni bir zafiyet bulunabilir. Yeni bir saldırı yöntemi ortaya çıkabilir. Bu nedenle siber güvenlik açısından “ürün tamamlandı” demek giderek anlamsızlaşmaktadır. Ürün piyasaya çıktıktan sonra da zafiyetlerin izlenmesi, değerlendirilmesi, gerekli yamaların geliştirilmesi, güncellemelerin güvenli biçimde dağıtılması ve yeni risklerin yeniden analiz edilmesi gerekmektedir.

Avrupa Birliği’nde bu yaklaşım, tıbbi cihaz düzenlemelerinin içine doğrudan yerleşmiş durumdadır. MDR (EU 2017/745 - Tıbbi Cihazlar Yönetmeliği) ve IVDR (EU 2017/746 - Vücut Dışında Kullanılan Tanı Amaçlı Tıbbi Cihaz Yönetmeliği) kapsamındaki siber güvenlik beklentilerini açıklayan MDCCG 2019-16 Rev.1 (Tıbbi Cihazlar İçin Siber Güvenlik Kılavuzu) rehberi, siber güvenliği tasarımdan ürün sonrası gözetim faaliyetlerine kadar uzanan bir yaşam döngüsü konusu olarak ele almaktadır. Rehber; güvenli tasarım, risk yönetimi, güvenlik doğrulaması, kullanım ortamı, ürün sonrası zafiyetlerin izlenmesi ve güvenlik güncellemeleri arasında bağlantı kurmaktadır. Bu açıdan MDR/IVDR düzenleyici beklentiyi tanımlarken, TS EN IEC 81001-5-1 bu beklentinin yazılım yaşam döngüsünde sistematik mühendislik faaliyetlerine dönüştürülmesine yardımcı olan önemli araçlardan biri olarak görülebilir.

Avrupa’daki çerçeve artık cihazın kendisiyle de sınırlı değildir. NIS2 (Ağ ve Bilgi Güvenliği) Direktifi sağlık kuruluşlarının kurumsal siber dayanıklılığını güçlendirirken, Avrupa Sağlık Veri Alanı (EHDS) Tüzüğü (EU 2025/327) elektronik sağlık verilerinin ve elektronik sağlık kayıt sistemlerinin daha güvenli ve birlikte çalışabilir bir ekosistem içinde ele alınmasına yönelik yeni bir katman oluşturmaktadır. Cihaz, yazılım, hastane ağı, sağlık verisi ve hizmet sağlayıcı böylece ayrı siber güvenlik

adaları olmaktan çıkıp aynı dijital sağlık ekosisteminin parçaları haline gelmektedir.

ABD’de de benzer bir yaşam döngüsü yaklaşımı gelişmektedir. Federal Gıda, İlaç ve Kozmetik Yasası Bölüm 524B kapsamında 29 Mart 2023’ten itibaren belirli “siber cihaz” başvurularında üreticilerin ürün sonrası zafiyetleri izleme ve ele alma planı sunması, güvenli geliştirme ve bakım süreçleri oluşturması, gerekli güncelleme ve yamaları sağlayabilmesi ve bir yazılım malzeme listesi (SBOM) sunması beklenmektedir. FDA’nın Şubat 2026 tarihli güncel ürün öncesi siber güvenlik rehberi de cihaz tasarımı, kalite yönetim sistemi ve başvuru dokümantasyonunu aynı yaşam döngüsü yaklaşımı içinde ele almaktadır. Avrupa ve ABD’nin düzenleyici araçları farklı olsa da ortak yön açıktır: siber güvenlik, piyasaya arzdan önce yapılan tek seferlik bir test değil, ürünün tüm yaşam döngüsü boyunca yönetilmesi gereken bir mühendislik sorumluluğudur.



Şekil 3 – Güvenli Tıbbi Cihaz Yaşam Döngüsü

TS EN 62304’ten TS EN IEC 81001-5-1’e: Güvenli Çalışan Yazılımdan Güvenli Kalabilen Yazılıma

Tıbbi cihaz yazılımı geliştirenler TS EN 62304 (Tıbbi cihaz yazılımı - Yazılım yaşam döngüsü süreçleri) standardını uzun zamandır bilmektedir. TS EN 62304 standardı bize yazılımın yaşam döngüsünü nasıl kontrollü yöneteceğimizi anlatırken, TS EN IEC 81001-5-1 standardı ise bu yapıya başka bir bakış açısı getirmektedir. Basitleştirerek söylersek:

- **TS EN 62304:** Yazılım doğru ve güvenli biçimde geliştiriliyor mu?

- **TS EN IEC 81001-5-1:** Yazılım değişen siber tehdit ortamında güvenli kalabilecek şekilde geliştiriliyor ve sürdürülebiliyor mu?

Bu nedenle iki standardı birbirinden bağımsız görmek yerine aynı ürün yaşam döngüsünün tamamlayıcı parçaları olarak düşünmek daha doğrudur. TS EN ISO 14971 (Tıbbi cihazlar - Tıbbi cihazlara risk yönetiminin uygulanması) standardının risk yönetimi yaklaşımı da bu yapıya eklenince önemli bir bağlantı ortaya çıkıyor: **Siber güvenlik artık yalnızca verinin gizliliği değil; belirli durumlarda doğrudan klinik riskin başlangıç noktası olabilir.** Örneğin bir infüzyon pompasının ağ bağlantısındaki güvenlik açığı, teorik olarak tedavi parametresine yetkisiz erişime; bu da yanlış doz gibi hasta emniyetini etkileyebilecek bir duruma dönüşebilir. Böyle bir senaryoda “siber güvenlik” ile “emniyet” arasındaki çizgi ortadan kalkmaya başlamaktadır.

Tıbbi Cihazın Güvenli Olması Yetmez; Güvenli Kalabilmesi Gerekir

TS EN IEC 81001-5-1 standardının belki de en önemli mesajı burada yatmaktadır. Geleneksel ürün güvenliği büyük ölçüde cihazın piyasaya çıktığı andaki durumuna odaklanabiliyordu. Siber güvenlik ise zamana bağlıdır. Bugün güvenli olan bir yazılım yarın yeni bir zafiyet nedeniyle güvenli olmayabilir. Bu yüzden modern tıbbi cihaz üreticisinin cevaplaması gereken soru artık yalnızca: “Ürünümüz güvenli mi?” değildir. Asıl soru şudur: “Ürünümüz değişen tehditler karşısında güvenli kalabilecek şekilde tasarlandı mı?” TS EN IEC 81001-5-1 bu soruya sistematik bir mühendislik yaklaşımı getirmektedir. MDR/IVDR ve MDCC rehberleriyle Avrupa’da, FDA’nın yaşam döngüsü temelli beklentileriyle ABD’de görülen düzenleyici yönelim de aynı ihtiyacı güçlendirmektedir. Sağlık teknolojileri daha bağlantılı, daha yazılım yoğun ve daha otonom hale geldikçe bu yaklaşımın önemi daha da artacaktır. **Çünkü geleceğin tıbbi cihazlarında güvenlik yalnızca doğru çalışan sensörler, güvenilir elektronik devreler veya hatasız algoritmalar anlamına gelmeyecektir. Güvenli bir tıbbi cihaz, aynı zamanda kendisini dijital dünyaya karşı koruyabilen ve yeni tehditlere uyum sağlayabilen bir sistem olmak zorundadır.**

KAYNAKLAR

1. *TS EN IEC 81001-5-1:2021, Sağlık yazılımı ve sağlık bilgi teknolojisi sistemlerinin emniyeti, etkinliği ve güvenliği - Bölüm 5-1: Güvenlik - Ürün yaşam döngüsündeki faaliyetler. Düzeltilmiş sürüm 2025-12; Yorum Belgesi 1:2025.*
2. *TS EN 62304:2006+A1:2015, Tıbbi cihaz yazılımı - Yazılım yaşam döngüsü süreçleri.*
3. *TS EN ISO 14971:2019, Tıbbi cihazlar - Tıbbi cihazlara risk yönetiminin uygulanması.*
4. *Avrupa Parlamentosu ve Konseyi. Tıbbi cihazlara ilişkin (MDR) (AB) 2017/745 sayılı Tüzük, özellikle Ek I - Genel Güvenlik ve Performans Gereklilikleri.*
5. *Avrupa Parlamentosu ve Konseyi. İn vitro tanısal tıbbi cihazlara ilişkin (IVDR) (AB) 2017/746 sayılı Tüzük, özellikle Ek I - Genel Güvenlik ve Performans Gereklilikleri.*
6. *Tıbbi Cihaz Koordinasyon Grubu (MDCC). MDCC 2019-16 Rev.1 - Tıbbi Cihazlar için Siber Güvenlik Kılavuzu, Temmuz 2020.*
7. *Avrupa Parlamentosu ve Konseyi. Birlik genelinde yüksek bir ortak siber güvenlik düzeyine yönelik tedbirler hakkında (AB) 2022/2555 sayılı Direktif (NIS2 Direktifi).*
8. *Avrupa Parlamentosu ve Konseyi. Avrupa Sağlık Veri Alanı (EHDS) hakkındaki (AB) 2025/327 sayılı Tüzük.*
9. *Avrupa Komisyonu. Hastaneler ve Sağlık Hizmeti Sağlayıcılarının Siber Güvenliğine İlişkin Avrupa Eylem Planı, 2025; 2025-2026 uygulama materyalleri.*
10. *ABD Gıda ve İlaç İdaresi (FDA). Tıbbi Cihazlarda Siber Güvenlik: Kalite Yönetim Sistemi Hususları ve Piyasaya Sürülmeden Önce Sunulacak Belgelerin İçeriği, Nihai Kılavuz, Şubat 2026.*
11. *ABD Gıda ve İlaç İdaresi (FDA). Contec ve Epsimed’e ait Bazı Hasta Monitörlerindeki Siber Güvenlik Açıkları: FDA Güvenlik Duyurusu, 30 Ocak 2025; 2 Temmuz 2025 tarihinde güncellenmiştir.*
12. *ABD Sağlık ve İnsan Hizmetleri Bakanlığı (HHS), Sivil Haklar Ofisi. Change Healthcare Siber Güvenlik Olayı Sık Sorulan Sorular, 2025 tarihinde güncellenmiştir.*
13. *ABD Sağlık ve İnsan Hizmetleri Bakanlığı (HHS), Sivil Haklar Ofisi. Dört HIPAA Güvenlik Kuralı Fidyeye Yazılımı Soruşturması, 23 Nisan 2026.*