

CCTV’de Güvenliđi NDAA ile Ölçmek Doğru mu?

Türkiye İçin Menş e Odaklı Değ il, Risk ve Siber Güvenlik Odaklı Bir Yaklaşım

“TURK IOT” Teknik değ erlendirme ve görüş yazısı • Eylül 2026

Kamu güvenliđi, kritik altyapı ve kurumsal güvenlik projelerinde IP kameralar, NVR’lar, VMS platformları ve diğ er ağ bağırlantılı fiziksel güvenlik cihazları artık yalnızca görüntü üreten ekipmanlar deđildir. Bu cihazlar; işletim sistemi, web servisi, API, ONVIF, RTSP, bulut bağırlantıları, mobil uygulamalar, üçüncü taraf kütüphaneler ve güncelleme mekanizmaları bulunan birer ağ bilgisayarıdır. Dolayısıyla satın alma kriterlerinin de yalnızca marka, menş e veya belirli bir yabancı ülkenin kamu alım mevzuatına uyumluluk beyanı üzerinden deđil, ürünün gerçek saldırı yüzeyi ve yaşam döngüsü boyunca nasıl yönetildiđi üzerinden kurulması gerekir.

Bu tartışmada sık karşılaşılan kavramlardan biri ABD National Defense Authorization Act (NDAA) ve özellikle Section 889 kapsamındaki kısıtlamalardır. Türkiye’de bazı CCTV şartnamelerinde “NDAA uyumlu” olma şartının doğrudan bir siber güvenlik kriteri gibi kullanıldığı görölmektedir. Oysa bu iki kavram aynı şeyi ifade etmez.

1. Önce Kavramı Doğru Tanımlayalım: NDAA Ne Söyler?

NDAA, tek başına “ürünün içinde hiçbir Çin menş eli komponent bulunmadığını” belgeleyen genel bir siber güvenlik sertifikası deđildir. ABD Federal Acquisition Regulation (FAR) 52.204-25 kapsamında Section 889 uygulaması; Huawei ve ZTE tarafından üretilen belirli telekomünikasyon ekipmanlarını, ayrıca kamu güvenliđi, kamu tesislerinin güvenliđi, kritik altyapının fiziksel güvenlik gözetimi ve benzeri ulusal güvenlik amaçları bakımından Hytera, Hikvision ve Dahua tarafından üretilen belirli video gözetim/telekomünikasyon ekipman ve hizmetlerini ve ilgili bağırlı kuruluşları hedefleyen bir federal tedarik kısıtlamasıdır.

Dolayısıyla NDAA uyumluluđu ile “siber güvenli ürün” kavramını eşitlemek teknik olarak doğru deđildir. Bir cihaz NDAA açısından uygun olabilir ve yine de uzaktan kod çalıştırma, kimlik doğrulama atlatma, zayıf parola politikası, güvensiz API, güncelleme zinciri problemi veya başka bir CVE’ye sahip olabilir. Tersı yönde de, NDAA kapsamındaki bir üreticinin belirli bir ürünü teknik açıdan güçlü güvenlik kontrolleri barındırabilir; fakat ABD federal tedarik politikası nedeniyle yine de kapsam dışında tutulabilir. Bunlar farklı risk kategorileridir.

2. Türkiye Açısından Sorulması Gereken Soru Farklıdır

Türkiye’de bir kamu kurumu veya kritik altyapı işletmecisi için temel soru “Bu ürün ABD federal satın alma politikasına uygun mu?” olmamalıdır. Asıl soru şudur: “Bu ürün, bizim tehdit modelimiz altında ne kadar güvenlidir; tedarik zinciri ne kadar şeffaftır; güvenlik açıkları nasıl yönetilmektedir ve cihaz ele geçirildiğinde oluşabilecek risk nasıl sınırlandırılmaktadır?”

Yabancı bir ülkenin ulusal güvenlik ve tedarik politikasının kendi bağlamında gerekçeleri olabilir. Ancak bu politikanın teknik bağlamından kopararak Türkiye’de doğrudan ürün

güvenliği ölçütü haline getirilmesi, güvenlik açısından sahte bir güven duygusu oluşturabileceği gibi satın alma süreçlerinde rekabeti de gereksiz biçimde daraltabilir.

Türkiye'nin ihtiyacı, belirli ülke veya marka isimlerini merkeze alan tek boyutlu bir filtre yerine; aynı kuralların tüm üreticilere uygulandığı, ölçülebilir, denetlenebilir ve teknik kanıta dayalı bir ürün güvenliği rejimidir.

3. Menşe Bilgisi Güvenlik Analizinin Bir Parçasıdır; Tamamı Değildir

Bir ürünün hangi ülkede üretildiği, hangi şirket tarafından tasarlandığı, firmware'in kim tarafından geliştirildiği ve kritik bileşenlerin nereden tedarik edildiği önemlidir. Özellikle kritik altyapılarda tedarik zinciri riski göz ardı edilemez. Ancak menşe bilgisi tek başına bir ürünün güvenli veya güvensiz olduğunu kanıtlamaz.

Modern CCTV ürünleri SoC, sensör, bellek, ağ PHY'si, güvenli element, işletim sistemi, açık kaynak kütüphaneler, web sunucusu, codec bileşenleri ve üreticiye özel uygulamalardan oluşur. Nihai risk, bütün bu katmanların birlikte değerlendirilmesiyle anlaşılabilir.

Bu nedenle satın alma süreçlerinde yalnızca "Made in X", "NDAA compliant" veya benzeri etiketlere bakmak yerine üreticiden ürün seviyesinde tedarik zinciri şeffaflığı, mümkünse SBOM, firmware imza mekanizması, secure boot bilgisi, güvenlik güncelleme politikası, destek süresi ve güvenlik açığı bildirim süreci istenmelidir.

4. "NDAA Uyumlu" Demek "Siber Güvenli" Demek Değildir

Siber güvenlik statik bir özellik değildir. Bir ürün bugün bilinen kritik bir açığa sahip olmayabilir; yarın yeni bir CVE yayımlanabilir. Bu nedenle güvenli ürün kavramını "hiç açığı olmayan ürün" şeklinde tanımlamak gerçekçi değildir.

Microsoft Security Response Center ve Cisco Security Advisories gibi büyük üreticilerin kamuya açık güvenlik programları incelendiğinde, dünyanın en büyük teknoloji şirketlerinin ürünlerinde de düzenli olarak güvenlik açıklarının tespit edildiği, CVE'lerin yayımlandığı ve yamaların veya azaltıcı önlemlerin geliştirildiği görülür. Bu durum tek başına üreticinin güvensiz olduğunu göstermez. Aksine, olgun bir güvenlik yaklaşımının önemli göstergelerinden biri güvenlik açığını kabul edebilmek, araştırmacılarla çalışmak, etkilenen sürümleri açıklamak ve zamanında düzeltme yayımlamaktır.

Dolayısıyla değerlendirilmesi gereken yalnızca "açık var mı?" sorusu değildir. "Üretici açığı nasıl keşfediyor, nasıl kabul ediyor, ne kadar hızlı düzeltiyor, müşteriyi nasıl bilgilendiriyor ve ürünün destek ömrü boyunca bu süreci sürdürüyor mu?" soruları en az bunun kadar önemlidir.

5. Türkiye İçin Daha Gerçekçi Bir CCTV Siber Güvenlik Modeli

Türkiye'de özellikle kamu, savunma, enerji, ulaştırma, finans, telekom ve kritik altyapı projelerinde ürün kabulünün teknik testlere bağlanması daha anlamlıdır. Burada tek bir "uygun/uygun değil" etiketi yerine katmanlı bir değerlendirme modeli uygulanabilir.

- Bağımsız laboratuvar güvenlik değerlendirmesi: Ürünün yetkin ve akredite laboratuvarlarda penetrasyon testi ve güvenlik değerlendirmesine tabi tutulması.
- Firmware ve backdoor analizi: Firmware'in statik/dinamik analizi; gizli hesaplar, hard-coded credential, undocumented servisler, beklenmeyen outbound bağlantılar, debug arayüzleri ve yetkisiz uzaktan erişim mekanizmalarının araştırılması.
- Zaafiyet analizi: Web arayüzü, API, ONVIF, RTSP, SSH/Telnet, SNMP, P2P/bulut protokolleri, mobil uygulama ve cihazın kullandığı üçüncü taraf bileşenlerin test edilmesi.
- Tedarik zinciri şeffaflığı: Üretici, üretim ülkesi, kritik SoC/bileşenler, firmware geliştirme sorumluluğu, OEM/ODM ilişkileri ve mümkünse SBOM bilgilerinin doğrulanması.
- Güvenli önyüklemeye ve firmware bütünlüğü: Secure Boot, imzalı firmware, rollback koruması ve güncelleme paketlerinin doğrulanması.
- Kimlik ve erişim güvenliği: Varsayılan parola bulunmaması, güçlü parola politikası, rol bazlı erişim, sertifika yönetimi, MFA desteği bulunan yönetim katmanları ve brute-force koruması.
- Şifreleme: HTTPS/TLS, sertifika doğrulama, güvenli anahtar saklama ve gerekli protokollerde güncel kriptografik yöntemler.
- Vulnerability Disclosure Policy: Üreticinin PSIRT/CERT benzeri güvenlik açığı bildirim kanalı, koordineli açıklama süreci ve yayımlanmış güvenlik duyuruları.
- Güncelleme ve destek politikası: Güvenlik yamalarının hangi süre boyunca sağlanacağı, kritik açıkların giderilme hedef süreleri ve EOL/EOS politikasının satın alma öncesinde açıklanması.
- Periyodik yeniden test: Ürün yalnızca ihaleye girişte değil; önemli firmware değişiklikleri, kritik CVE'ler veya belirli periyotlar sonrasında tekrar değerlendirilmelidir.

6. TSE ve Akredite Test Yaklaşımı

Türkiye'de bu yapının ulusal standart ve akreditasyon sistemi üzerinden kurgulanması mümkündür. TSE'nin Ortak Kriterler (Common Criteria) ekosistemi ve ISO/IEC 15408 ailesi, BT ürünlerinin güvenlik özelliklerinin değerlendirilmesi için uluslararası bir çerçeve sunar. TSE yayınlarında Ortak Kriterler kapsamında çalışan laboratuvarlar için ISO/IEC 17025 akreditasyonu gibi şartlardan söz edilmektedir.

Ancak CCTV için pratik satın alma modeli yalnızca Common Criteria sertifikasına indirgenmemelidir. Kamera ve NVR gibi sürekli değişen firmware'e sahip IoT cihazlarında ürün-spesifik penetrasyon testi, firmware analizi, ağ davranışı analizi, CVE/SBOM kontrolü ve yeniden test mekanizması birlikte düşünülmelidir.

Bu nedenle şartnamelerde "TSE A seviyesi" gibi kurum içi veya sektörel bir ifade kullanılacaksa bunun hangi resmi akreditasyon/sertifikasyon kapsamına karşılık geldiği açıkça tanımlanmalıdır. Teknik şartname, laboratuvarın hangi standarda göre akredite olacağını ve hangi test kapsamının uygulanacağını doğrudan yazmalıdır.

7. Güvenlik Yalnızca Ürünle Sağlanmaz

En güvenli kamera bile yanlış ağ mimarisinde risk oluşturabilir. CCTV sistemleri mümkün olduğunca ayrı VLAN/VRF üzerinde konumlandırılmalı, internete doğrudan çıkış engellenmeli, yalnızca gerekli hedeflere ve portlara erişim verilmelidir. Yönetim erişimi ayrı yönetim ağından yapılmalı; firewall, NAC, IDS/IPS/NDR, SIEM ve merkezi loglama gibi kontroller sistemin önem derecesine göre devreye alınmalıdır.

Cihazın DNS sorguları, outbound bağlantıları, başarısız oturum açmaları, konfigürasyon değişiklikleri ve olağan dışı trafik davranışları izlenebilmelidir. Böylece güvenlik yalnızca satın alma anındaki bir sertifikaya değil, sistemin tüm işletme ömrüne yayılan sürekli bir kontrole dönüşür.

8. “Hiç Açığı Olmayan Ürün” Yerine “Açığını Yönetebilen Ekosistem”

Sıfır güvenlik açığı garantisi gerçekçi değildir. Güvenlik açığı, karmaşık yazılım ve donanım sistemlerinin doğal risklerinden biridir. Kritik olan; bilinçli olarak bırakılmış arka kapıların önlenmesi, güvenli geliştirme süreçlerinin uygulanması, açığın hızlı tespit edilmesi, şeffaf biçimde duyurulması, düzeltmenin yayımlanması ve kurumların bu düzeltmeyi zamanında uygulayabilmesidir.

NIST’in IoT üreticileri için yayımladığı güncel rehber de ürün güvenliğini yalnızca satış öncesi bir kontrol olarak görmez; üreticinin ürünün yaşam döngüsü boyunca güvenlik kabiliyetleri, bakım, destek, güvenlik açığı bildirimi, güncelleme ve müşteriye bilgi sağlama süreçlerini ele alır. Bu yaklaşım CCTV için de daha gerçekçi bir referans modelidir.

9. Kamu İhalelerinde Nasıl Bir Şartname Daha Sağlıklı Olur?

Menşe veya tek bir yabancı mevzuat uyumluluğunu güvenliğin yerine koymak yerine aşağıdaki gibi üreticiden bağımsız bir model tercih edilebilir:

- Ürün, tanımlanmış kapsamda bağımsız siber güvenlik testinden geçmiş olmalıdır.
- Test raporu ürünün tam modelini, donanım revizyonunu ve firmware sürümünü belirtmelidir.
- Kritik ve yüksek seviye bulgular için giderim ve yeniden doğrulama süreci bulunmalıdır.
- Hard-coded parola, gizli kullanıcı, belgelenmemiş uzaktan yönetim servisi ve yetkisiz backdoor bulunmadığı test edilmelidir.
- Ürünün internet erişimi olmadan temel fonksiyonlarını sürdürebilmesi ve gereksiz bulut bağımlılıklarının kapatılabilmesi değerlendirilmelidir.
- Üretici güvenlik açığı bildirim politikası ve güvenlik güncelleme taahhüdü sunulmalıdır.
- SBOM veya eşdeğer üçüncü taraf bileşen envanteri, kritik projelerde talep edilebilmelidir.
- Firmware imzalama, secure boot ve güncelleme bütünlüğü mekanizmaları doğrulanmalıdır.
- OEM/ODM ve kritik tedarik zinciri ilişkileri beyan edilmeli; menşe ve üretici bilgileri gerektiğinde bağımsız doğrulamaya açık olmalıdır.
- Kurum ağı tarafında segmentasyon, erişim kontrolü, merkezi loglama ve anomali izleme zorunlulukları proje tasarımına dahil edilmelidir.

Sonuç: Etiketten Çok Kanıta İhtiyacımız Var

NDAA, ABD’nin kendi ulusal güvenlik ve federal tedarik politikası içinde değerlendirilmesi gereken bir düzenlemedir. Türkiye’nin ise kendi risklerini, kritik altyapılarını, tedarik zincirini ve siber güvenlik ihtiyaçlarını esas alan teknik bir değerlendirme mekanizmasına ihtiyacı vardır.

Bir CCTV ürününün güvenli olup olmadığını yalnızca “NDAA compliant” etiketiyle belirlemek yeterli değildir. Aynı şekilde yalnızca üretim ülkesine bakarak güvenlik kararı vermek de eksik kalır. Gerçek güvenlik; bağımsız test, firmware ve backdoor analizi, tedarik zinciri şeffaflığı, güvenli güncelleme, CVE yönetimi, üretici sorumluluğu, ağ segmentasyonu ve sürekli izleme gibi kontrollerin birlikte uygulanmasıyla oluşur.

Daha sağlıklı yaklaşım, “hangi ülkeden geliyor?” sorusunu tamamen terk etmek değil; onu “ürün gerçekte kim tarafından geliştiriliyor ve üretiliyor, hangi bileşenleri kullanıyor, hangi ağ davranışlarını gösteriyor, hangi güvenlik kontrollerine sahip ve bir açık bulunduğunda ne oluyor?” sorularıyla tamamlamaktır.

Türkiye’de kamu ve kritik altyapı CCTV projelerinde hedef, yabancı bir tedarik mevzuatını kopyalamak yerine kendi teknik güvenlik standardımızı oluşturmak olmalıdır. Rekabeti marka veya ülke isimleri üzerinden değil, ölçülebilir güvenlik gereksinimleri üzerinden kurmak; hem daha adil hem de siber güvenlik açısından daha savunulabilir bir sonuç üretir.

Kaynaklar ve Teknik Referanslar

- **U.S. FAR 52.204-25 - Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment**
<https://www.acquisition.gov/far/52.204-25>
- **FCC - Section 889 / Covered List bağlamı**
<https://www.fcc.gov/supplychain/coveredlist>
- **NIST IR 8259 Rev. 1 - Foundational Cybersecurity Activities for IoT Product Manufacturers (2026)**
<https://csrc.nist.gov/pubs/ir/8259/r1/final>
- **NIST IoT Device Cybersecurity Requirement Catalogs**
<https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/>
- **ISO/IEC 15408-1:2026 - Evaluation criteria for IT security**
<https://www.iso.org/standard/15408-1>
- **Microsoft Security Response Center**
<https://www.microsoft.com/en-us/msrc>
- **Cisco Security Advisories**
<https://sec.cloudapps.cisco.com/security/center/publicationListing.x>