CRA EVİDENCE TEKNİK DOKÜMANI

AB Siber Dayanıklılık Tüzüğü: pratik uyum rehberi

Dijital unsurlu ürünlerin imalatçıları, ithalatçıları ve dağıtıcıları için teknik doküman.

Hazırlayan	CRA Evidence
Sürüm	1.1
Durum	Yaşayan belge
Dayanak	AB Tüzüğü 2024/2847

Değişiklik geçmişi

Bu, yaşayan bir belgedir. Komisyon kılavuzları, uyumlaştırılmış standartlar ve CRA kapsamında pazar uygulaması geliştikçe güncellenir.

Sürüm	Tarih	Açıklama
1.0	17 Mayıs 2026	İlk yayın. Kapsam, sınıflandırma, esaslı değişiklik, temel gereklilikler, güvenlik açığı yönetimi, teknik dosya, uygunluk değerlendirmesi yollarını ve AI Act, Veri Yasası, ESPR ile ürün sorumluluğu mevzuatıyla ilişkiyi kapsar.
1.1	6 Kasım 2026	Komisyonun Temmuz 2026 rehberi ve 11 Eylül 2026'dan beri uygulanan Madde 14 bildirimi eklendi.

İçindekiler

Özet 4

Siber Dayanıklılık Tüzüğü nedir? 5

Uyum planlaması için kritik tarihler 6

Hangi ürünler kapsamda 8

Esaslı değişiklik: yeniden uygunluk ne zaman gerekir 15

Hazır bulundurmanız gerekenler 18

- Siber güvenlik risk değerlendirmesi 18
- Destek süresi belirlemesi 19
- Bileşen durum tespiti 19
- 13 ürün güvenliği gerekliliği 20
- 8 güvenlik açığı yönetimi gerekliliği 21
- Madde 14 bildirim zaman çizelgeleri 21
- Ürün uygunsuz olduğunda düzeltici aksiyon 23
- Ürün belgeleri gereklilikleri 25
- Uygunluk değerlendirmesi rotası kontrol listesi 25

Ürün güvenliği gereklilikleri 27

Güvenlik açığı yönetimi gereklilikleri 31

Teknik dosyada bulunması gerekenler 34

- Teknik belgeler 34
- AB Uygunluk Beyannamesi 35
- Kullanıcı bilgileri ve talimatları 36

Doğru uygunluk değerlendirmesi rotasını seçme 37

- Modül A: öz değerlendirme 37
- Modül B ve C: ürün odaklı değerlendirme 37
- Modül H: süreç odaklı değerlendirme (tam kalite güvencesi) 37

CRA'nın daha geniş AB mevzuat çerçevesindeki yeri 39

CRA Evidence nasıl yardımcı olur 40

Özet

60 SANİYEDE

Kapsam: AB pazarına arz edilen bağlantılı donanım ve yazılım ürünleri. Siber güvenlik, iyi uygulama başlığı olmaktan çıkar ve ürün uyumu gerekliliği hâline gelir.

İlk etkisi: Madde 14 bildirimleri 11 Eylül 2026'dan beri uygulanıyor. Tam teknik dosya, belgeler ve CE işareti yükümlülükleri 11 Aralık 2027'den itibaren uygulanır.

Hazırlamanız gerekenler: siber güvenlik risk değerlendirmesi, SBOM, teknik dosya, kullanıcı talimatları, AB Uygunluk Beyannamesi, CE işareti ve Madde 14 olay/güvenlik açığı bildirimleri.

Kim harekete geçmeli

Ana yük imalatçıdadır. İthalatçı ve dağıtıcıların ürünleri sunmadan önce özen kontrolleri vardır.

Ne değişiyor

Siber güvenlik ürün uyumunun parçası olur: güvenli tasarım, güvenlik açığı yönetimi, belgeler, CE işareti ve piyasaya arz sonrası aksiyon.

Şimdiden uygulanıyor

Madde 14 bildirimi, aktif olarak istismar edilen güvenlik açıkları ve ağır olaylar için **11 Eylül 2026**'dan itibaren uygulanıyor.

Tam uygulama

Tam teknik uyum **11 Aralık 2027** tarihinde uygulanır. Önceki ürünler esaslı değişiklik sonrası kapsama girer, ancak bildirim yükümlülüğü devam eder.

Kanıt omurgası

Teknik dosyada risk değerlendirmesi, SBOM, destek süresi gerekçesi, test kanıtı, talimatlar, beyanname ve temel siber güvenlik gerekliliklerine uygunluk kanıtı yer alır.

Uygunluk rotası

Çoğu ürün Modül A öz değerlendirmesini kullanabilir. Önemli ve Kritik ürünlerde Onaylanmış Kuruluş veya AB siber güvenlik sertifikasyonu gerekebilir.

Siber Dayanıklılık Tüzüğü nedir?

(AB) 2024/2847 sayılı Siber Dayanıklılık Tüzüğü (CRA), AB pazarına arz edilen dijital unsurlu ürünler için siber güvenliği bağlayıcı bir gereklilik hâline getiren ilk yatay AB çerçevesidir. Bağlayıcı metin EUR-Lex üzerindedir.

CRA, bağlantılı donanım ve yazılımların imalatçılarına, ithalatçılarına ve dağıtıcılarına uygulanır. Tüketici IoT cihazlarından endüstriyel kontrol sistemlerine kadar geniş bir ürün alanını kapsar. Pratik değişiklik nettir: siber güvenliğin ürün uyumunun parçası olarak tasarlanması, kanıtlanması, sürdürülmesi ve izlenmesi gerekir.

Temel siber güvenlik gerekliliklerine veya Madde 13 ve 14 yükümlülüklerine uyumsuzluk, hangisi daha yüksekse 15 milyon EUR'ya veya küresel yıllık cironun %2,5'ine kadar idari para cezasına yol açabilir. Daha düşük basamaklar da uygulanır: belirtilen diğer yükümlülüklerin ihlali için 10 milyon EUR'ya veya %2'ye kadar; onaylanmış kuruluşlara veya piyasa gözetim otoritelerine yanlış, eksik veya yanıltıcı bilgi sağlanması için 5 milyon EUR'ya veya %1'e kadar. Piyasa gözetim ve denetim otoriteleri ayrıca düzeltici aksiyon, arzın sınırlandırılması, ürünün piyasadan çekilmesi veya geri çağırma da isteyebilir.

Uyum planlaması için kritik tarihler

CRA **10 Aralık 2024**'te yürürlüğe girdi. Pratik uyum çalışması üç ana tarihe odaklanır: **Haziran 2026**'da Onaylanmış Kuruluş kuralları, **Eylül 2026**'da bildirimler ve **Aralık 2027**'de tam teknik uyum.

NOT

Komisyon rehberinin güncel durumu: Avrupa Komisyonu 27 Temmuz 2026'da C(2026) 5252 sayılı CRA rehberinin içeriğini yayımladı. Rehber, Mart 2026 istişare taslağının yerini aldı. Bağlayıcı değildir ve resmî kabul, tüm dil sürümleri hazır olana kadar bekliyor. Piyasaya arz, özgür ve açık kaynak yazılım, destek süreleri, esaslı değişiklik, ürün sınıflandırması, bileşen durum tespiti, uzaktan veri işleme, güvenlik açığı yönetimi ve diğer AB mevzuatıyla kesişimler için planlama malzemesi olarak yararlıdır. AI Act ve DORA sınır konuları için ek rehber gerekebilir.

10 Aralık 2024

Yürürlük

Geçiş dönemi başlar

11 Haziran 2026

Onaylanmış Kuruluşlar

Bölüm IV uygulanır

11 Eylül 2026

Bildirim

Madde 14 bildirimleri uygulanır

11 Aralık 2027

Tam uygulama

Teknik gereklilikler, CE işareti, belgeler ve uygunluk değerlendirmesi

ÖNCE BUNU YAPIN

Önce bildirim hazırlığıyla başlayın. Madde 14 tarihi tam teknik uyumdan önce gelir ve hâlihazırda AB pazarında bulunan ürünlere de uygulanır.

Bildirimler **11 Eylül 2026**'dan beri uygulandığı için ilk uygulama iş akışı bildirim hazırlığı olmalıdır: **tespit, sınıflandırma, kullanıcı bildirimi ve otorite bildirimi** şimdiden, tam teknik uyum tarihinden önce çalışır durumda olmalıdır.

11 Aralık 2027'den önce piyasaya arz edilen dijital unsurlu ürünler, bu tarihten itibaren **esaslı değişiklik** geçirmedikçe CRA'nın teknik gerekliliklerine tabi olmaz. Madde 14 bildirimi farklıdır. Kapsamdaki tüm ürünlere uygulanır; buna 11 Aralık 2027'den önce AB pazarında bulunan ürünler de dahildir.

Ürün yaşam döngüsünde CRA

ADIM 01

Ürün kapsamını belirle

Kapsam, sınıflandırma, destek süresi ve risk değerlendirmesi

ADIM 02

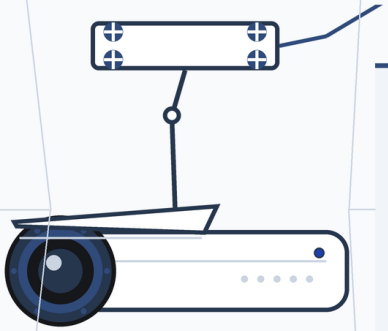
Güvenli geliştir

Güvenli varsayılanlar, kod analizi, SBOM ve bağımlılık kontrolü

ADIM 03

Doğrula ve belgele

Güvenlik testleri, zafiyet triyajı, teknik dosya ve kullanıcı talimatları



ADIM 04

Piyasaya sun

AB uygunluk beyanı, CE işareti ve yayın kararı

ADIM 05

İzle ve güncelle

CVE'ler, duyurular, exploit faaliyeti, güvenlik güncellemeleri ve açıklama

ADIM 06

Destekle ve iş birliği yap

Madde 14 bildirimi, kullanıcı uyarıları, otorite talepleri ve destek sonu

Bağlı IP kamera, ürün planlamasından CRA kapsamında piyasa sonrası desteğe kadar

Hangi ürünler kapsamda

Kapsam ve istisnalar

CRA, amaçlanan veya makul olarak öngörülebilir kullanımı bir cihaza ya da ağa doğrudan veya dolaylı veri bağlantısı içeren donanım ve yazılım ürünlerine uygulanır. Buna bilgisayarlar, akıllı telefonlar, ağ ekipmanları, IoT cihazları, endüstriyel kontrol sistemleri ve veri işleme uygulamaları dahildir.

Aşağıdaki kategoriler açıkça kapsam dışıdır:

- (AB) 2017/745 ve (AB) 2017/746 sayılı düzenlemeler kapsamındaki tıbbi cihazlar ve in vitro tanı cihazları
- (AB) 2019/2144 sayılı düzenleme kapsamındaki otomotiv sistemleri
- (AB) 2018/1139 sayılı düzenleme kapsamındaki havacılık ekipmanları
- 2014/90/AB sayılı Direktif kapsamındaki denizcilik ekipmanları
- Yalnızca ulusal güvenlik veya savunma amaçları için geliştirilen ürünler
- Dijital unsur veya ağ bağlantısı içermeyen tamamen mekanik ürünler

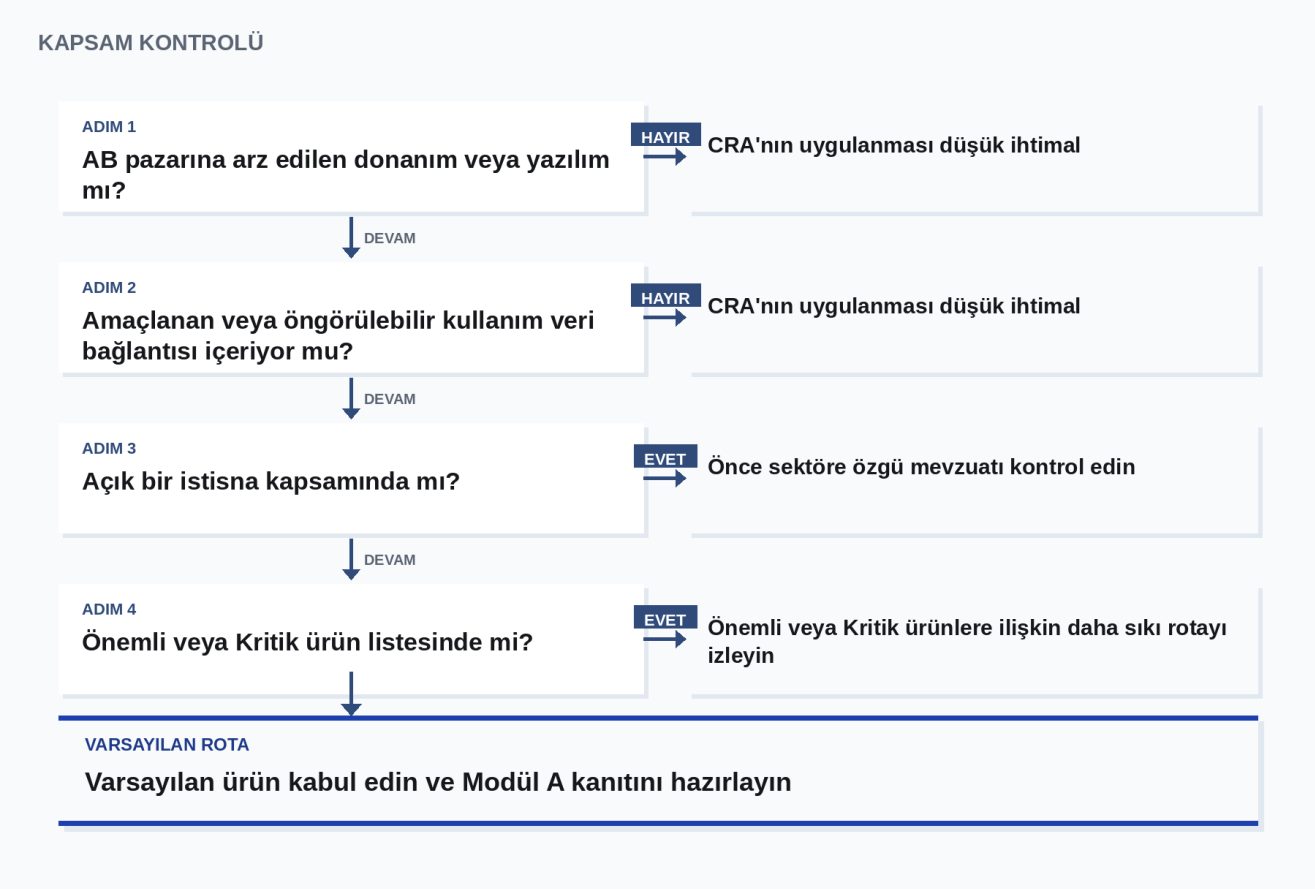
Açık bir istisna yoksa, bağlantılı ürününüzü kapsamda kabul edin.

NOT

Özel olarak hazırlanmış ürünler: dar bir istisna. Tek bir ticari kullanıcıya, sizinle o kullanıcı arasında yazılı bir sözleşmeyle özel olarak hazırlanan bir ürün için yalnızca iki gereklilikten sapabilirsiniz: güvenli varsayılan yapılandırma (ürünün orijinal güvenli durumuna dönmesi için bir yol yine de sunulmalıdır) ve ücretsiz güvenlik güncellemeleri (sözleşme farklı bir ticari esas belirleyebilir). Diğer her şey tam olarak uygulanır: güvenlik açığı yönetimi, diğer ürün güvenliği gereklilikleri, Madde 14 bildirimi, teknik dosya, CE işareti, uygunluk değerlendirmesi ve destek süresi. Bu genel bir B2B istisnası değildir; işletmelere satılan hazır ürünleri kapsamaz.

EKONOMIK OPERATÖR SORUMLULUKLARI

İmalatçı	Güvenli ürün tasarlar, riski değerlendirir, teknik dosyayı hazırlar, uygunluk değerlendirmesini yürütür, güvenlik açıklarını yönetir, Madde 14 olaylarını bildirir.
İthalatçı	İmalatçı uyumunu kontrol eder, CE işaretini ve belgeleri doğrular, beyannameyi erişilebilir tutar, bilinen güvenlik açıklarında aksiyon alır.
Dağıtıcı	Arz öncesi özen göstergelerini kontrol eder, gerekli bilgi ve talimatları doğrular, uyumsuz ürünleri piyasaya sunmaz.



Ürün sınıflandırması değerlendirme rotasını belirler

Ürün kategoriniz, uygunluğu nasıl göstereceğinizi belirler.

Kategori	Örnekler	Uygunluk değerlendirmesi
Varsayılan "Sınıflandırılmamış"	Önemli veya Kritik kategorilerde yer almayan genel yazılım ve bağlantılı tüketici ürünleri	Modül A: öz değerlendirme
Önemli "Sınıf I"	Kimlik, tarayıcı, parola yöneticisi, antivirüs, VPN, ağ yönetimi, yönlendirici, akıllı kilit, güvenlik kamerası ve benzeri ürünler	Modül A yalnızca uygulanabilir uyumlaştırılmış standartlar, ortak spesifikasyonlar veya sertifikasyon şemaları gerekli şekilde uygulanıyorsa; aksi halde Modül B+C veya Modül H
Önemli "Sınıf II"	Hipervizörler, konteyner çalışma zamanları, güvenlik duvarları, IDS/IPS ve kurcalamaya dayanıklı mikroişlemciler	Modül B+C, Modül H veya en az "substantial" güvence düzeyinde uygulanabilir Avrupa siber güvenlik sertifikasyon şeması
Kritik ürünler	Güvenli elemanlar, akıllı kartlar, akıllı sayaç ağ geçitleri ve donanım güvenlik kutuları	Gerekli ve mevcut olduğunda Avrupa siber güvenlik sertifikasyonu; aksi halde Sınıf II rotaları uygulanır

Dört ürün kategorisi

Yukarıdaki tablo örnekleri gösterir. Ürününüzün temel işlevini karşılaştırdığınız tam liste aşağıdadır.

Varsayılan ürünler

Çoğu ürün burada yer alır. Temel işlevi aşağıdaki Önemli veya Kritik listelerden hiçbiriyle eşleşmeyen dijital unsurlu ürünler Varsayılan kabul edilir. Uygunluk rotası Modül A öz değerlendirmesidir.

Yaygın örnekler:

- Akıllı TV'ler ve yayın akış cihazları.
- Ağ yazıcıları ve çok işlevli ofis cihazları.
- Bluetooth hoparlörler ve tüketici ses ürünleri.
- Medya oynatıcı yazılım uygulamaları.
- Oyun konsolları, e-okuyucular ve benzeri tüketici elektroniği.
- Güvenlik işlevi olmayan akıllı mutfak aletleri: fırın, buzdolabı, bulaşık makinesi.
- Güvenlik işlevi olmayan akıllı ampuller ve bağlantılı aydınlatma.
- Sağlık izleme amacı olmayan fitness takipçileri.
- Tarayıcı, parola yöneticisi veya VPN uygulaması olmayan genel amaçlı mobil uygulamalar.
- Kelime işlemci ve hesap tablosu gibi ofis verimlilik yazılımları.

Yukarıdaki liste örneklendirme amaçlıdır. Aşağıdaki Önemli ve Kritik listeler kapsayıcıdır.

Önemli ürünler (Sınıf I)

Uygulanabilir uyumlaştırılmış standartlar, ortak spesifikasyonlar veya sertifikasyon şemaları gerekli şekilde uygulanmadığı sürece zorunlu üçüncü taraf değerlendirmesi.

1. Kimlik yönetimi ve ayrıcalıklı erişim yönetimi yazılımı ve donanımı, biyometrik okuyucular dahil kimlik doğrulama ve erişim kontrol okuyucuları.
2. Bağımsız ve gömülü tarayıcılar.
3. Parola yöneticileri.
4. Kötü amaçlı yazılım arayan, kaldıran veya karantinaya alan yazılımlar.
5. VPN ürünleri.
6. Ağ yönetim sistemleri.
7. Güvenlik bilgi ve olay yönetimi (SIEM) sistemleri.
8. Önyükleme yöneticileri.
9. Açık anahtar altyapısı ve dijital sertifika veren yazılımlar.
10. Fiziksel ve sanal ağ arayüzleri.
11. İşletim sistemleri.
12. Yönlendiriciler, internete bağlanmak üzere tasarlanmış modemler ve anahtarlar.
13. Güvenlikle ilgili işlevleri olan mikroişlemciler.
14. Güvenlikle ilgili işlevleri olan mikrodenetleyiciler.
15. Güvenlikle ilgili işlevleri olan ASIC ve FPGA'lar.

16. Akıllı ev genel amaçlı sanal asistanlar.
17. Güvenlik işlevleri olan akıllı ev ürünleri: akıllı kapı kilitleri, güvenlik kameraları, bebek izleme sistemleri, alarm sistemleri.
18. Etkileşimli özellikleri olan internete bağlı oyuncaklar: konuşma, görüntü kaydı, konum takibi.
19. Sağlık izleme amaçlı kişisel giyilebilir cihazlar (Tüzük (AB) 2017/745 veya 2017/746 uygulanmadığında) veya çocukların kullanımına yönelik giyilebilir cihazlar.

Önemli ürünler (Sınıf II)

Zorunlu üçüncü taraf değerlendirmesi, daha sıkı rota. Uyumlaştırılmış standartlar mevcut olsa bile öz değerlendirme kullanılamaz.

1. İşletim sistemlerinin ve benzeri ortamların sanallaştırılmış çalıştırılmasını destekleyen hipervizörler ve konteyner çalışma zamanı sistemleri.
2. Güvenlik duvarları, saldırı tespit ve önleme sistemleri.
3. Kurcalamaya dayanıklı mikroişlemciler.
4. Kurcalamaya dayanıklı mikrodenetleyiciler.

Kritik ürünler

Şemanın mevcut olduğu durumlarda Avrupa siber güvenlik sertifikasyonu gerekir. Aksi halde Sınıf II rotası uygulanır.

1. Güvenlik kutuları bulunan donanım cihazları.
2. (AB) 2019/944 sayılı Direktif'in 2. maddesi 23. noktasında tanımlanan akıllı sayaç sistemleri içindeki akıllı sayaç ağ geçitleri ve güvenli kriptografik işleme dahil ileri güvenlik amaçları için diğer cihazlar.
3. Akıllı kartlar ve benzeri cihazlar, güvenli elemanlar dahil.

Ürününüzün temel işlevi Önemli veya Kritik listelerinde yer alan bir maddeyle eşleşiyorsa, ürün o sınıftadır. Ürününüz bu maddelerden birini bir bileşen olarak entegre ediyor ancak kendi temel işlevi başka bir şeyse, entegrasyon sınıfınızı değiştirmez).

Nasıl sınıflandırılır: temel işlev, entegrasyon değil

Yukarıdaki listeler kategorilerin ne olduğunu söyler. Bunları ürününüze nasıl uygulayacağınızı söylemez. CRA'nın yanıtı tek bir terimdir: **temel işlev**.

Sınıfınız, ürününüzün temel işlevinin ne olduğuyla belirlenir, hangi bileşenleri entegre ettiğiyle değil. Temel işlevi Önemli listelerle eşleştirin, ürün Önemli (Sınıf I veya Sınıf II) olur. Kritik listeyle eşleştirin, ürün Kritik olur. Hiçbiriyle eşleşmezse Varsayılan olur. Testin tamamı budur ve 8(1)).

Pratik güvence Madde 7(1)'in ikinci cümlesinde yer alır. Önemli bir bileşeni entegre etmek, entegre eden ürünü Önemli sınıfına itmez. Bir akıllı ev hub'ına güvenlik duvarı kütüphanesi gömmek, hub'ı güvenlik duvarı yapmaz. Resital 45 bunu sade biçimde ortaya koyar: güvenlik duvarları ve saldırı tespit sistemleri Önemli Sınıf II'dir, ancak bunları entegre eden diğer ürünler değildir.

Öz sınıflandırma için şu adımları kullanın.

1. **Ürününüzün temel işlevini tek cümlede adlandırın.** Bunu yapamıyorsanız analizin geri kalanı çöker. Ürünün onsuz çalışamayacağı şeye odaklanın.
2. **Yukarıdaki Önemli listeleri kontrol edin.** Sınıf I veya II'de eşleşme ürünü Önemli yapar.
3. **Yukarıdaki Kritik listeyi kontrol edin.** Eşleşme ürünü Kritik yapar. Şemanın mevcut olduğu durumlarda Avrupa siber güvenlik sertifikasyon rotası uygulanır; aksi halde Sınıf II rotası uygulanır.
4. **Hiçbir listede eşleşme yok.** Ürün Varsayılandır. Rota Modül A öz değerlendirmesidir.
5. **Gerekçeyi belgeleyin.** Temel işlev cümlesini, liste kontrolünü ve seçilen rotayı içeren tek sayfalık bir not teknik dosyaya girer.

İki çalışılmış örnek.

Gömülü parola yöneticisi olan akıllı ev hub'ı. Temel işlev: evdeki tüketici IoT cihazları arasında rutinleri koordine etmek. Kendi imalatçısı tarafından ayrı satılan parola yöneticisi bileşeni başlı başına bir Önemli Sınıf I ürünüdür. Hub'ın temel işlevi kimlik bilgisi yönetimi değil, ev otomasyonudur. Hub Varsayılan olarak kalır.

Özellik kümesine göre işletim sistemi. Bir ürün akıllı ev aleti olarak pazarlanır, ancak ana işlevleri donanım ve çevre birimi başlatma, süreç zamanlama, bellek yönetimi ve bir sistem çağrı arayüzüdür. Bu, bir işletim sisteminin temel işlevidir. İşletim sistemleri Önemli Sınıf I ürünüdür. Pazarlama ne derse desin ürün Önemli Sınıf I'dir.

Sınıflandırmanız ekibin geri kalanını şaşırtan bir sınıfa düşerse, temel işlev cümlesinin yayından önce bir kez daha gözden geçirilmesi gerekir.

Bulut ürününüzün bir parçası olduğunda

Çoğu dijital unsurlu ürün, cihaz dışında bir şeye yaslanır: bulut arka uç, mobil eşlik uygulaması, kablosuz güncelleme sunucusu, kimlik doğrulama portalı, cihaz yönetim sistemi. CRA bunların hepsini ürününüz olarak görmez. Bunları yalnızca iki koşul birden sağlandığında ürünün parçası olarak görür):

- Yazılım **sizin ekibiniz tarafından veya sizin sorumluluğunuzda tasarlanmış ve geliştirilmiş**tir.
- Ürün, bu yazılım olmadan **işlevlerinden birini yerine getiremez**.

Bu koşullardan biri sağlanmıyorsa, uzak hizmet CRA için ürün sınırının dışında kalır. Sahibi olmadığınız üçüncü taraf bir SaaS, ürününüz onunla konuşsa bile, ürününüzün parçası değildir. Ürünü tanıtan ancak işlevlerini desteklemeyen bir web sitesi de ürünün parçası değildir (Resital 12).

Bir uzak bileşen kapsamdaysa, **ürünün bir parçası olarak** kapsamdadır. Teknik dosya, uygunluk değerlendirmesi, AB Uygunluk Beyannamesi, güvenlik açığı yönetimi ve Madde 14 bildirim süreleri bulut bileşenini cihazla birlikte kapsar.

Konuyu hızla netleştirmek için bu matrisi kullanın.

Bileşen	Ürünün parçası olarak kapsamda mı?
Cihazla eşleşen mobil eşlik uygulaması	**Evet.** Siz tasarladınız, cihaz onsuz kurulamaz veya kullanılamaz.
Cihazın verisini saklayan ve işleyen bulut arka uç	**Evet.** Siz tasarladınız, panel veya ana özellik onsuz çalışmaz.
Kablosuz güncelleme sunucusu	**Evet.** Siz tasarladınız, cihaz onsuz güvenlik güncellemesi alamaz.
Cihaza erişimi kontrol eden kimlik doğrulama portalı	**Evet.** Siz tasarladınız, kullanıcılar onsuz oturum açamaz.
Ürünün pazarlama web sitesi	**Hayır.** Bir ürün işlevini desteklemez.
Ürünün entegre olduğu üçüncü taraf SaaS (sahibi siz değilsiniz)	**Hayır.** Siz tasarlamadınız. Üçüncü taraf sağlayıcı NIS 2 kapsamında kendi yükümlülüklerini taşır.
Hizmetinizin üzerinde çalıştığı genel bulut altyapısı (IaaS veya PaaS)	**Hayır.** Siz tasarlamadınız. Altyapı sağlayıcısı NIS 2 kapsamındadır.

Yaygın bir örüntü: mobil uygulaması, güncelleme sunucusu ve bulut arka ucu olan bir akıllı ev cihazı. Üçü de imalatçı tarafından tasarlanmıştır ve cihaz reklamı yapılan işlevlerini onlar olmadan yerine getiremez. Üçü de ürünün parçasıdır. CRA yükümlülükleri tüm bu paket için geçerlidir. Bulut arka uç daha sonra üçüncü taraf bir analitik SaaS ile konuşuyorsa, o SaaS ürünün parçası değildir. Üçüncü taraf sağlayıcı NIS 2 kapsamında kendi yükümlülüklerini taşır.

CRA, imalatçının ağ ve bilgi sistemleri için bir bütün olarak güvenlik önlemleri talep etmez. Ürünün parçası olan uzak hizmetler için güvenlik talep eder (Resital 11). Sınır şirket sınırı değil, ürün sınırıdır.

Tedarik zinciriniz: CRA kapsamında kim ne yapar

CRA ana yükümlülükleri size, yani imalatçıya yükler, ancak ithalatçı ve dağıtıcıların da ürününüzün pazara nasıl ulaştığını etkileyen görevleri vardır. Bilmeniz gereken üç şey önemlidir.

Kim	Arz öncesi neyi doğrular	Güvenlik açığında ne yapar	Sizin görevlerinizi ne zaman üstlenir
İthalatçı	CE işareti, AB Uygunluk Beyannamesi, doğru dilde kullanıcı talimatları, ürün üzerinde veya ürünle birlikte iletişim bilgileriniz	Gereksiz gecikme olmadan size haber verir; ürün önemli bir siber güvenlik riski sunuyorsa piyasa gözetim ve denetim otoritelerine doğrudan haber verir	Ürününüzü kendi adı veya markası altında piyasaya arz ettiğinde ya da üründe esaslı değişiklik yaptığında
Dağıtıcı	CE işareti, sizin ve ithalatçının yapması gerekenleri yaptığı, gerekli belgelerin ürünle birlikte sunulduğu	Gereksiz gecikme olmadan size haber verir; ürün önemli bir siber güvenlik riski sunuyorsa piyasa gözetim ve denetim otoritelerine doğrudan haber verir; ürünü piyasaya sunmayı durdurabilir	İthalatçılarla aynı tetikleyici

Bir imalatçı için bu üç pratik anlama gelir:

- CE işaretiniz, AB Uygunluk Beyannameniz ve kullanıcı talimatlarınız, bir dağıtıcı kontrol ettiği anda doğru ve doğru dilde olmalıdır. Kanal ortakları bunları doğrulamakla yükümlüdür ve eksik veya hatalıysa ürünü piyasaya sunmayı reddedebilir.
- İthalatçılar ve dağıtıcıların güvenlik açıklarını sizin güvenlik açığı yönetimi sürecinize bildirebileceği açık, sürtünmesiz bir iletişim yolu sağlamanız gerekir. Bu yolu kullanacaklar.
- Ürününüzü yeniden markalayan, kendi adı veya markası altında piyasaya arz eden veya esaslı şekilde değiştiren her ortak, o sürüm için imalatçı hâline gelir. Tam teknik dosya, uygunluk değerlendirmesi, bildirim ve destek süresi görevleri o sürüm için onlara geçer. Esaslı değişiklik kuralı için bir sonraki bölümdeki *Başka biri imalatçı hâline geldiğinde* alt başlığına bakın.

Esaslı değişiklik: yeniden uygunluk ne zaman gerekir

Ürününüz pazara çıktıktan sonra CRA, sonraki değişiklikleri iki gruba ayırır. Çoğu rutindir ve ek hiçbir şey gerektirmez. Bazıları esaslıdır. Esaslı bir değişiklik, CRA açısından pazara yeni bir ürün arz ediliyormuş gibi ele alınır. Bu, yeni bir uygunluk değerlendirmesi, güncellenmiş bir teknik dosya, yeni bir AB Uygunluk Beyannamesi ve yeni sürümde CE işareti anlamına gelir.

Test kısadır ve esaslı değişiklik tanımında yer alır). Şu iki koşuldan biri doğruysa değişiklik esaslıdır:

- Temel siber güvenlik gerekliliklerine **uygunluğu etkiliyorsa**.
- Ürünün değerlendirildiği **amaçlanan kullanımı değiştiriyorsa**.

Hiçbiri uygulanmazsa değişiklik esaslı değildir. Gerekçeyi yine de belgeleyin ve dosyada tutun. Analiz, kanıt zincirinin parçasıdır.

Esaslı sayılmayanlar

İki istisna pratikte işin çoğunu yapar.

Amaçlanan kullanımı değiştirmeden siber güvenlik riskini azaltan güvenlik güncellemeleri ve hata düzeltmeleri esaslı değildir (Resital 39). Bilinen bir güvenlik açığına yama yapmak, bir hatayı kapatmak için girdi doğrulamasını ayarlamak veya bir CVE'yi gidermek için bileşeni yeniden derlemek hep bu tarafta yer alır.

Yenileme, bakım ve onarım da otomatik olarak esaslı değildir (Resital 42). Yalnızca amaçlanan kullanımı değiştirir veya temel siber güvenlik gerekliliklerine uygunluğu etkilerse esaslı hâle gelir.

Küçük arayüz çalışması da güvenli tarafta kalır. Bir dil eklemek, bir simge setini değiştirmek veya ekran düzenini cilalamak tek başına esaslı bir değişiklik değildir. Yeterli girdi doğrulaması gerektiren yeni bir girdi öğesi eklemek esaslı olabilir (Resital 39).

Yedek parçalar

CRA, yedek parçaları dar ve belirli biçimde muaf tutar. **Aynı spesifikasyonlara göre üretilen özdeş yedek parçalar**, değiştirdikleri bileşenlerle aynı şekilde, Tüzüğün kapsamı dışındadır. İşlevsel ikameler değildir.

Konuyu hızla netleştirmek için bu matrisi kullanın.

Değiştirme	Ana ürün 11 Aralık 2027'den önce piyasaya arz edildi	Ana ürün 11 Aralık 2027'de veya sonrasında piyasaya arz edildi
Orijinal bileşenle **özdeş**, aynı spesifikasyon	Yedek parça CRA kapsamı dışında. Değişim hiçbir yükümlülük tetiklemez.	Yedek parça CRA kapsamı dışında. Değişim hiçbir yükümlülük tetiklemez.
İşlevsel olarak eşdeğer, farklı tasarım veya spesifikasyon	Yedek parça başlı başına CRA ürünüdür. Ana ürünün CRA yükümlülüğü yoktur, çünkü uygulama tarihinden öncedir.	Yedek parça CRA ürünüdür. Yedek parçayı ana ürüne takmanın yukarıdaki iki ayaklı testle ana ürünün esaslı değişikliği olup olmadığını değerlendirin.

İki pratik sonuç. Birincisi, muafiyet özdeş spesifikasyona bağlıdır. Farklı bir yonga seti üzerine yeniden üretilmiş bir kablosuz modül, müşteri farkı anlamasa bile özdeş yedek parça değildir. İkincisi, işlevsel ikame sağlayan imalatçı, ana ürünü kim yapmış olursa olsun, o parça için CRA yükümlülüklerini taşır.

Yazılım güncellemeleri ve özellik anahtarları

Yazılım sürümleri, esaslı değişiklik sorularının en yaygın kaynağıdır. İki ayaklı test bunları da çözer.

Bir güvenlik açığını gideren yama esaslı değildir. Ürünün hiç değerlendirilmediği bir yeteneği açan bir özellik anahtarı esaslıdır. Ürünün yeni girdi kategorileri hakkında karar vermesini sağlayan bir model yükseltmesi de esaslıdır. Bir sürüm hem bir düzeltme hem yeni bir özellik içeriyorsa, özelliği değerlendirin.

Paketleme, özden daha az önemlidir. Bir özellik güncellemesinin tek başına mı yoksa bir güvenlik yamasıyla aynı sürümde mi geldiği değerlendirme açısından önemsizdir (Resital 39).

Özellik anahtarları veya kademeli yayınlama kullanıyorsanız, sayılan an, anahtarı içeren binary'nin gönderildiği an değil, üretimde son kullanıcılar için etkinleştirildiği andır.

Pratikte karar

Yayına çıkmadan önce her değişikliği şu sırayla değerlendirin.

1. **Değişiklik ürünün amaçlanan kullanımını değiştiriyor mu?** Evet ise: esaslı. Yeni sürüm için uygunluk değerlendirmesini tekrar yürütün.
2. **Değişiklik temel siber güvenlik gerekliliklerine uygunluğu etkiliyor mu?** Evet ise: esaslı. Yeni sürüm için uygunluk değerlendirmesini tekrar yürütün.
3. **Aksi takdirde:** esaslı değil. Analizi belgeleyin ve mevcut teknik dosya altında devam edin.

Ürün Önemli veya Kritik sınıftaysa ve rota ilk seferinde üçüncü taraf değerlendirmesi gerektiriyorsa, esaslı bir değişiklik sizi aynı rotaya geri koyar. Esaslı olması muhtemel her değişiklikten önce üçüncü tarafa haber verin. Öz değerlendirme, Önemli bir ürünü sonradan yeniden sınıflandırmak için bir arka kapı değildir.

Bir değişiklik esaslı olduğunda sonuçlar

Esaslı bir değişiklik, pazara yeni bir ürün arz ediliyormuş gibi ele alınır. İmalatçı için bu şu anlama gelir:

- Değişen sürüm için teknik dosyayı güncelleyin.
- Uygunluk değerlendirmesini ürün sınıfının gerektirdiği rotada tekrar yürütün.
- Değiştirilen sürüm için yeni bir AB Uygunluk Beyannamesi düzenleyin.
- CE işaretini yeniden iliştirin, yeni beyanname dosyada olsun.
- Önceki sürümün belgelerini tam saklama süresi boyunca tutun. Yeni sürüm onu silmez.

Özellikle yazılım ürünleri için, eski sürümlerin kullanıcıları yeni sürüme ücretsiz olarak ve yeni donanım gerekmeden geçebildiği sürece, destek süresi boyunca güvenlik güncellemelerini pazara sunduğunuz en son sürümle sınırlayabilirsiniz.

Önceki uygunluk altında satılan saha birimleri etkilenmez. Yükümlülük, değiştirilen sürümün piyasaya sunulmasına bağlanır, ondan önceki özdeş birimlere değil.

Başka biri imalatçı hâline geldiğinde

Asıl imalatçı değilseniz ve esaslı bir değişiklik yapıyorsanız, CRA o sürüm için sizi imalatçı olarak görür. Madde 13 ve 14'ün tüm yükümlülükleri size bağlanır. Aynı kural, ürünü kendi adınız veya markanız altında piyasaya arz ettiğinizde de geçerlidir.

Bu, ekiplerin genellikle beklediğinden daha fazla durumu yakalar:

- Yeni özelliklerle müşteriye özel bir gömülü yazılım sürümü gönderen bir sistem entegratörü.
- Bir ürünü white-label'layan ve pazarlanan amaçlanan kullanımı değiştiren bir bayi.
- Üçüncü taraf bir cihazı kendi gömülü yazılımıyla paketleyen bir hizmet sağlayıcı.

Her durumda, değişikliği yapan aktör o sürüm için imalatçı yükümlülüklerini devralır: teknik dosya, uygunluk değerlendirmesi, bildirim, güvenlik açığı yönetimi ve geri kalanı. Her iki sınırı geçtiği anda "ithalatçı" veya "dağıtıcı" etiketi onu korumayı bırakır.

Hazır bulundurmanız gerekenler

Bu bölümü çalışma kontrol listesi olarak kullanın. Gereklilik bazındaki ayrıntılı rehberlik sonraki bölümlerde yer alır.

Siber güvenlik risk değerlendirmesi

Ürünü piyasaya arz etmeden önce teknik dosyada bir siber güvenlik risk değerlendirmesi bulunmalıdır. Bu, ürünün neden güvenle pazara sunulabileceğini ve pazarda kalabileceğini kendi sözlerinizle açıklayan belgedir.

Değerlendirme şunları kapsamalıdır:

- Ürünün amaçlanan kullanımı ve makul olarak öngörebileceğiniz kullanım senaryoları
- Ürünün çalışacağı koşullar ve ortam
- Korunması gereken veri ve işlevler
- Geçerli tehditler ve bunları yönetmek için kullandığınız kontroller
- Ürünün kullanımda kalması beklenen süre

Çoğu ekibin nasıl yapılandırdığı. Güvenilir metodolojiler aynı adımlarda birleşir: varlıkları belirleyin (ürünün işlediği veriler, anahtarlar ve kimlik bilgileri gibi güvenlik unsurları, kaybı kullanıcılara zarar verecek işlevler), her varlığın nerede bulunduğunu veya hareket ettiğini eşleyin, tehditleri varlık ve ortam bazında gizlilik, bütünlük ve erişilebilirlik boyutlarını kullanarak modelleyin, etki ve olasılığı puanlayın, hangi artık riskleri kabul edeceğinize ve hangilerini azaltacağınıza karar verin, ardından her kontrol turundan sonra yeniden değerlendirin (her yeni anahtar, sertifika veya kimlik doğrulama işlevi kendi başına analiz edilmesi gereken yeni bir varlıktır).

Tehdit modelleme. Yukarıdaki üçüncü adım en teknik harekettir ve kendi yerleşik teknikleri vardır. STRIDE tehditleri kimliğe bürünme (spoofing), kurcalama (tampering), inkâr (repudiation), bilgi ifşası (information disclosure), hizmet reddi (denial of service) ve yetki yükseltme (elevation of privilege) olarak sınıflandırır; yaygındır, çoğu bağlantılı ürüne uyar. LINDDUN kişisel veriyi işleyen ürünler için resmi genişletir: bağlanabilirlik, tanımlanabilirlik, inkâr edilemezlik, tespit edilebilirlik, bilgi ifşası, farkındasızlık ve uyumsuzluk; veri koruma rejiminin CRA görevleriyle örtüştüğü yerlerde yararlıdır. PASTA, iş hedeflerinden artık risk kabulüne uzanan yedi aşamalı bir süreç işletir; saldırı tablosunun tasarımı yönlendirdiği karmaşık sistemler için yararlıdır. Bunların hiçbiri CRA'ya özel değildir ve CRA bunlardan birini gerektirmez. Ürününüzün maruziyet profiline uyanı seçin.

Çalışılmış bir metodoloji nerede bulunur. CRA bir yöntem öngörmez. Almanya Federal Bilgi Güvenliği Ofisi (BSI) Teknik Kılavuz TR-03183'ü yayımlar; kamuya açık dolaşımdaki en ayrıntılı CRA uyumlu risk değerlendirmesi metodolojisidir. ENISA daha geniş CRA uygulama rehberi yayımlar.

Değerlendirmeyi destek süresi boyunca güncel tutun. Tehdit tablosu, bileşenler veya kullanım senaryosu değiştiğinde değerlendirme de onlarla değişmelidir.

Destek süresi belirlemesi

Her ürünün tanımlanmış bir destek süresi olmalıdır ve bitiş tarihini satın alma anında yayımlamanız gerekir. Destek süresi, güvenlik açıklarını yönettiğiniz, güvenlik güncellemeleri gönderdiğiniz ve teknik dosyayı güncel tuttuğunuz penceredir.

Ne kadar uzun olmalı

En az beş yıl. Ürünün beş yıldan az kullanılması bekleniyorsa destek süresi beklenen kullanım süresiyle eşleşmelidir. Daha uzun kullanılması bekleniyorsa destek süresi bu daha uzun kullanımı yansıtmalıdır; yönlendiriciler, işletim sistemleri ve endüstriyel kontrolörler gibi ürünler beş yıldan fazlasını rutin olarak hak eder.

Tartılacak etkenler

Süreyi belirlerken aşağıdakileri orantılı biçimde dikkate alın:

- Ürün için makul kullanıcı beklentileri
- Ürünün niteliği, amaçlanan kullanımı dahil
- Bu kategori için ürün ömrü belirleyen mevcut AB mevzuatı
- Pazardaki karşılaştırılabilir ürünlerin destek süreleri
- Ürünün bağlı olduğu işletim ortamının kullanılabilirliği
- Temel işlevleri sağlayan entegre bileşenlerin destek süreleri
- Ürün kategorisi için ADCO veya Komisyon rehberi

Seçilen sürenin gerekçesi teknik dosyada olmalıdır. Piyasa gözetim ve denetim otoriteleri talep edebilir.

Neyi yayımlamanız gerekiyor

Destek süresinin sonunu satın alma anında, en az ay ve yıl olarak, kolayca erişilebilir bir yerde belirtin. Ürünün kullanıcı arayüzü varsa, destek süresinin sonuna ulaştığında bir bildirim gösterin.

Güncelleme saklama

Destek süresi boyunca kullanıcılara sunulan her güvenlik güncellemesi, yayımlanmasından sonra en az 10 yıl veya destek süresinin kalan kısmı boyunca, hangisi daha uzunsa, erişilebilir kalmalıdır.

Bileşen durum tespiti

Ürün, bileşenlerden oluşur. Bir kısmını siz yazdınız, bir kısmını satın aldınız, bir kısmını açık kaynak depodan aldınız. CRA, uyum açısından ürünü bir bütün olarak ele alır, bu yüzden bileşenler de sayılır. Bir bileşende güvenlik açığı varsa, ürününüzde de vardır. Bir bileşen güvenlik güncellemesi almıyorsa, ürününüz de almıyor demektir.

İmalatçılar, açık kaynak olanlar dahil üçüncü taraf bileşenlere durum tespiti uygulamalıdır. Bileşenler ürünün siber güvenliğini tehlikeye atmamalıdır.

Ne kadar durum tespitinin yeterli olduğu, bileşenin taşıdığı siber güvenlik riskine bağlıdır. Kimlik doğrulama yapan bir kütüphane ile yazı tipi oluşturma kütüphanesi aynı değildir. Riske orantılı olarak şu kontrollerden bir veya birkaçını uygulayın:

1. **Bileşende CE işareti olup olmadığını kontrol edin.** Bileşenin kendisi bir CRA ürünüyse ve tedarikçi uygunluğu göstermişse, CE işareti bileşendedir. Bu, tedarikçinin kendi CRA çalışmasını gösterir.
2. **Güvenlik güncellemesi geçmişini kontrol edin.** Düzenli güvenlik güncellemesi yayımlayan bir bileşen, yıllardır sessiz olan birinden daha iyi bir risktir. Sürüm sıklığına ve yakın tarihli güvenlik duyurusu kaydına bakın.
3. **Bileşeni güvenlik açığı veri tabanlarına karşı kontrol edin.** Avrupa güvenlik açığı veri tabanı ve kamuya açık CVE veri tabanları bileşen hakkında bilinenleri size söyler. Yamasız bilinen bir CVE, kırmızı bayraktır.
4. **Ek güvenlik testleri çalıştırın.** Yukarıdakiler yeterli değilse, bileşeni entegrasyon bağlamınızda test edin: statik analiz, dinamik analiz, fuzzing veya odaklanmış güvenlik incelemesi.

Kendi tedarikçisi henüz tam olarak CRA kapsamında olmayan bileşenler için (henüz CE işareti yoksa), diğer üç kontrolü kullanın. Tedarik zinciri yetişmeye çalışıyor diye durum tespiti yükümlülüğü durmaz.

Dosyada tutulacak kanıt

Teknik dosyanın durum tespitinizi göstermesi gerekir, sadece iddia etmesi değil. Şunları tutun:

- Ürün içindeki üçüncü taraf bileşenlerin sürümlere izlenebilir listesi, açık kaynak olanlar dahil. SBOM, bunun doğal yeridir.
- İncelediğiniz tedarikçi güvenlik belgeleri: güvenlik politikaları, güvenlik açığı açıklama programları, destek süresi taahhütleri.
- Bileşenin ürününüzde güvenli şekilde davrandığını gösteren entegrasyon test raporları.
- Ticari tedarikçilerle yapılan sözleşme veya SLA'lardaki güvenlik maddeleri: güvenlik açığı bildirim süreleri, destek süresi taahhütleri, eskalasyon kuralları.
- Bileşen durum tespitinin sınırları ortaya çıkardığı yerlerde eklediğiniz ürün düzeyindeki azaltıcı önlemlerin kaydı: sandbox, kısıtlı izinler, girdi doğrulama, ağ segmentasyonu.

Bir bileşende güvenlik açığı bulduğunuzda

Durum tespitiniz veya piyasaya arz sonrası izlemeniz bir bileşende güvenlik açığı tespit ederse iki şey yapmalısınız. Birincisi, bileşeni sürdüren kişi veya kuruluşa haber verin. Bileşen açık kaynak ise, bu, üst akış projedir. İkincisi, kendi keşfettiğiniz herhangi bir güvenlik açığıyla aynı sürelerde güvenlik açığını ürününüzde ele alın ve giderin. Bir düzeltme geliştirdiyseniz, kodu veya belgeleri uygulanabilir olduğunda makine tarafından okunabilir bir formatta sürdürücüyle paylaşın.

CRA, kendi kullanıcılarınızı korumadan önce bileşen sürdürücünün eyleme geçmesini beklemenize izin vermez. Ürününüzün güvenlik açığı yönetimi süresi üst akıştan bağımsız işler.

13 ürün güvenliği gerekliliği

Her dijital unsurlu ürün, piyasaya arz edildiğinde ve destek süresi boyunca on üç temel güvenlik gerekliliğini karşılamalıdır. Bunlar, CRA kapsamında ürün açısından siber güvenliğin ne anlama geldiğinin tabanıdır.

On üç gereklilik şunlardır:

- Piyasaya arz anında bilinen istismar edilebilir güvenlik açığı bulunmaması
- Kutudan çıkar çıkmaz güvenli varsayılan yapılandırma
- Vazgeçme seçeneğiyle otomatik güncellemeler dahil güvenlik güncellemeleri
- Yetkisiz erişime karşı koruma
- Saklanan, aktarılan ve işlenen verinin gizliliği
- Veri, gömülü yazılım ve yapılandırma bütünlüğü
- Veri minimizasyonu
- Hizmet reddi saldırılarına karşı dahil erişilebilirlik ve dayanıklılık
- Diğer bağlı cihazlar veya ağlar üzerinde olumsuz etki yaratmama
- Dış arayüzler dahil sınırlı saldırı yüzeyi
- İstismar azaltma yoluyla olay etkisinin azaltılması
- Kullanıcının vazgeçme seçeneğiyle güvenlikle ilgili faaliyetlerin kayıt altına alınması
- Güvenli ve kalıcı veri silme ile taşınabilirlik

Her gereklilik rehberin ilerleyen kısımlarında pratikte ne anlama geldiği ve dosyada tutmanız gereken kanıtlarla birlikte ayrıntılı olarak açıklanır.

8 güvenlik açığı yönetimi gerekliliği

İmalatçıların ayrıca ürünün destek süresi boyunca çalışan güvenlik açığı yönetimi süreçlerine ihtiyacı vardır:

1. Güvenlik açıklarını belirleme ve belgeleme (SBOM dahil)
2. Risk yönetimi ve zamanında güvenlik güncellemeleri
3. Düzenli güvenlik testleri
4. Güvenlik güncellemeleri ve güvenlik açığı açıklamaları için bilgilendirme
5. Koordineli güvenlik açığı açıklama (CVD) politikası
6. Güvenlik açığı paylaşımı ve bildirim iletişim noktası
7. Güvenli güncelleme dağıtım mekanizmaları
8. Danışma mesajlarıyla ücretsiz güvenlik güncellemeleri

Madde 14 bildirim zaman çizelgeleri

Bu yükümlülükler **11 Eylül 2026**'dan itibaren uygulanır. Kapsamdaki dijital unsurlu ürünlerin imalatçılarına uygulanır; buna **11 Aralık 2027**'den önce piyasaya arz edilmiş ürünler de dahildir. Mikro ve küçük işletmeler bildirimden genel olarak muaf değildir. Küçük işletmelere yönelik ceza kolaylığı dardır: yalnızca ilk **24 saatlik erken uyarı süresi** ile ilgilidir.

CRA güvenlik açığı durumunu üç düzeyde ayırır:

- **Güvenlik açığı:** istismar edilebilecek herhangi bir zayıflık
- **İstismar edilebilir güvenlik açığı:** gerçek dünya koşullarında kullanılabilecek zayıflık
- **Aktif olarak istismar edilen güvenlik açığı:** bir saldırıda kullanıldığı doğrulanmış zayıflık

Sayaç ne zaman başlar

Bir sinyal geldiği anda saatte değilsiniz. Sayaç, ilk değerlendirmeyi yaptıktan ve ürününüzdeki bir güvenlik açığının aktif olarak istismar edildiğine ya da ağır bir olayın ürününüzün güvenliğini tehlikeye attığına dair makul derecede kesinliğe ulaştıktan sonra başlar. Vurgu, soruşturmanın tam olarak kapanmasını beklemekte değil, hızlı ilk değerlendirmededir. Bir müşteri, araştırmacı, otorite veya başka bir üçüncü taraf potansiyel bir konuyu dikkatinize sunarsa, gecikmeden değerlendirin ve değerlendirme size makul kesinliği verdiği anda sayacı başlatın.

Aktif olarak istismar edilen bir güvenlik açığı tespit ettiğinizde aşağıdaki bildirim zaman çizelgesi uygulanır:

Süre	Gereken bildirim	Bildirim yeri
24 saat içinde	Aktif istismara ilişkin erken uyarı bildirimi	Ulusal CSIRT üzerinden ENISA
72 saat içinde	Güvenlik açığı bildirimi: etkilenen ürün, istismar ve güvenlik açığının genel niteliği, azaltıcı önlemler, kullanıcıların alabileceği düzeltici önlemler ve gerekiyorsa hassasiyet işareti	Ulusal CSIRT üzerinden ENISA
Düzeltici veya azaltıcı önlemin mevcut olmasından en geç 14 gün sonra	Nihai rapor: güvenlik açığı açıklaması, ciddiyet, etki, kötü niyetli aktörlere ilişkin mevcut bilgiler ve güvenlik güncellemesi veya diğer düzeltici önlemlerin ayrıntıları	Ulusal CSIRT üzerinden ENISA

Ürün güvenliğini etkileyen **ağır bir olay** tespit ettiğinizde aşağıdaki bildirim zaman çizelgesi uygulanır:

Süre	Gereken bildirim	Bildirim yeri
24 saat içinde	Olayın hukuka aykırı veya kötü niyetli eylemlerden kaynaklandığından şüphelenilip şüphelenilmediğini de içeren erken uyarı bildirimi	Ulusal CSIRT üzerinden ENISA
72 saat içinde	Olay bildirimi: olayın niteliği, ilk değerlendirme, azaltıcı önlemler, kullanıcıların alabileceği düzeltici önlemler ve gerekiyorsa hassasiyet işareti	Ulusal CSIRT üzerinden ENISA
72 saatlik olay bildiriminden sonraki bir ay içinde	Nihai rapor: ayrıntılı olay açıklaması, ciddiyet, etki, muhtemel tehdit veya kök neden ve uygulanan ya da devam eden azaltıcı önlemler	Ulusal CSIRT üzerinden ENISA

Bildirimler öğrendikçe güncellenir

24 saatlik, 72 saatlik ve 14 günlük (veya bir aylık) gönderimler ayrı dosyalamalar değil, aynı bildirimin aşamalarıdır. Her aşama, bir önceki aşamada henüz mevcut olmayan bilgileri ekler. Koordinatör olarak belirlenen CSIRT herhangi bir anda ara güncelleme de isteyebilir. Daha önce verdiğiniz bilgileri tekrarlamanız gerekmez.

Bildirimler **CRA Tek Bildirim Platformu** üzerinden yapılır, imalatçının ana Üye Devletindeki ulusal Bilgisayar Güvenliği Olay Müdahale Ekibi (CSIRT) üzerinden yönlendirilir ve ENISA'ya eş zamanlı erişim sağlanır.

Kullanıcılarınızı bilgilendirme

Farkına vardıktan sonra, etkilenen kullanıcıları ve uygun olduğunda tüm kullanıcıları güvenlik açığı veya olay hakkında ve uygulayabilecekleri risk azaltma ve düzeltici önlemler hakkında bilgilendirmeniz gerekir. Bu, kamuya açıklamayla aynı şey değildir. Görev, kendilerini korumak için bilgiye ihtiyacı olan kullanıcılara bilginin

riskle orantılı biçimde ulaştırılmasıdır. Hassas veya kritik ortamlarda kullanılan ürünler için, güvenlik açığı azaltılmadığı sürece ayrıntılı teknik bilgiyi ilgili müşterilerle sınırlayın; erken kamu ayrıntısı istismarı kolaylaştırabilir.

Güvenlik açığı giderildikten veya azaltıldıktan sonra, kullanıcıların ürünlerinin artık etkilenmediğini doğrulamalarına ve genel farkındalığı artırmaya yardımcı olmak için daha geniş açıklama uygun hâle gelebilir. Ayrıntı düzeyini ve zamanlamayı artık riskle orantılı tutun. Kullanıcıları zamanında bilgilendirmezseniz, CSIRT bunu orantılı ve gerekli gördüğünde devreye girerek bilgiyi kendisi sağlayabilir.

Madde 14 bildirim zaman çizelgeleri

Aktif olarak istismar edilen güvenlik açığı	
24 saat	erken uyarı bildirimi
72 saat	güvenlik açığı bildirimi
düzeltici önlemden 14 gün sonra	nihai rapor

Ağır olay	
24 saat	erken uyarı bildirimi
72 saat	olay bildirimi
72 saatlik bildirimden bir ay sonra	nihai rapor

Ürün uygunsuz olduğunda düzeltici aksiyon

Piyasaya arz ettiğiniz bir ürünün veya süreçlerinizden birinin CRA temel siber güvenlik gerekliliklerine uygun olmadığını biliyor veya bunun için makul bir nedeniniz varsa, derhal harekete geçmeniz gerekir. Yükümlülük, piyasaya arzdan itibaren ve tüm destek süresi boyunca çalışır.

Üç seçenek

1. **Uygun hâle getirin.** Ürünü veya süreci düzeltin. Yazılım ürünleri için bu genellikle bir güvenlik güncellemesi veya süreç değişikliğidir. Düzeltmeyi desteklenen sürümlere uygulayın.
2. **Geri çekin.** Ürünü pazarda sunmayı bırakın. Tedarik zincirinizden ve stok tutan perakendeci, entegratör ve bayilerden çekin.

3. **Geri çağırın.** Hâlihazırda ürüne sahip kullanıcılardan ürünü geri alın. Kullanıcılara yönelik siber güvenlik riskinin önemli olduğu ve düzeltme ya da geri çekmenin tek başına yeterli olmadığı durumlarda kullanın.

Seçim sabit bir sıra değil, riskle orantılı bir karardır. Çalışan bir düzeltmesi olan yamanabilir bir güvenlik açığı genellikle *uygun hâle getirme* anlamına gelir. Sahada güvenle düzeltilemeyen bir ürün genellikle *geri çekme* ve önemli risk taşıyan aktif kullanımdaysa *geri çağırma* anlamına gelir.

Ayrıca yapmanız gerekenler

- Uygunsuzluk aktif olarak istismar edilen bir güvenlik açığı veya ağır bir olay olduğunda **Madde 14 zinciri kapsamında bildirim yapın**. Bildirim zaman çizelgesi yukarıda yer alır.
- **Kullanıcıları** uygunsuzluk ve kendilerinin uygulayabileceği düzeltici önlemler hakkında bilgilendirin. Orantılılık kuralları için yukarıdaki *Kullanıcılarınızı bilgilendirme* bölümüne bakın.
- Bir piyasa gözetim ve denetim otoritesinin gerekçeli her talebine, teknik belgeleri okuyabilecekleri bir dilde sağlamak dahil, **işbirliği** yapın.
- **Kanıtı koruyun.** Neyi bulduğunuzu, ne zaman bulduğunuzu, ne yaptığınızı ve kullanıcılar ile otoritelerle nasıl iletişim kurduğunuzu gösteren kayıtları tutun. Teknik belgeler ve AB Uygunluk Beyannamesi, piyasaya arzdan sonra en az 10 yıl veya tam destek süresi boyunca, hangisi daha uzunsa, erişilebilir kalmalıdır.

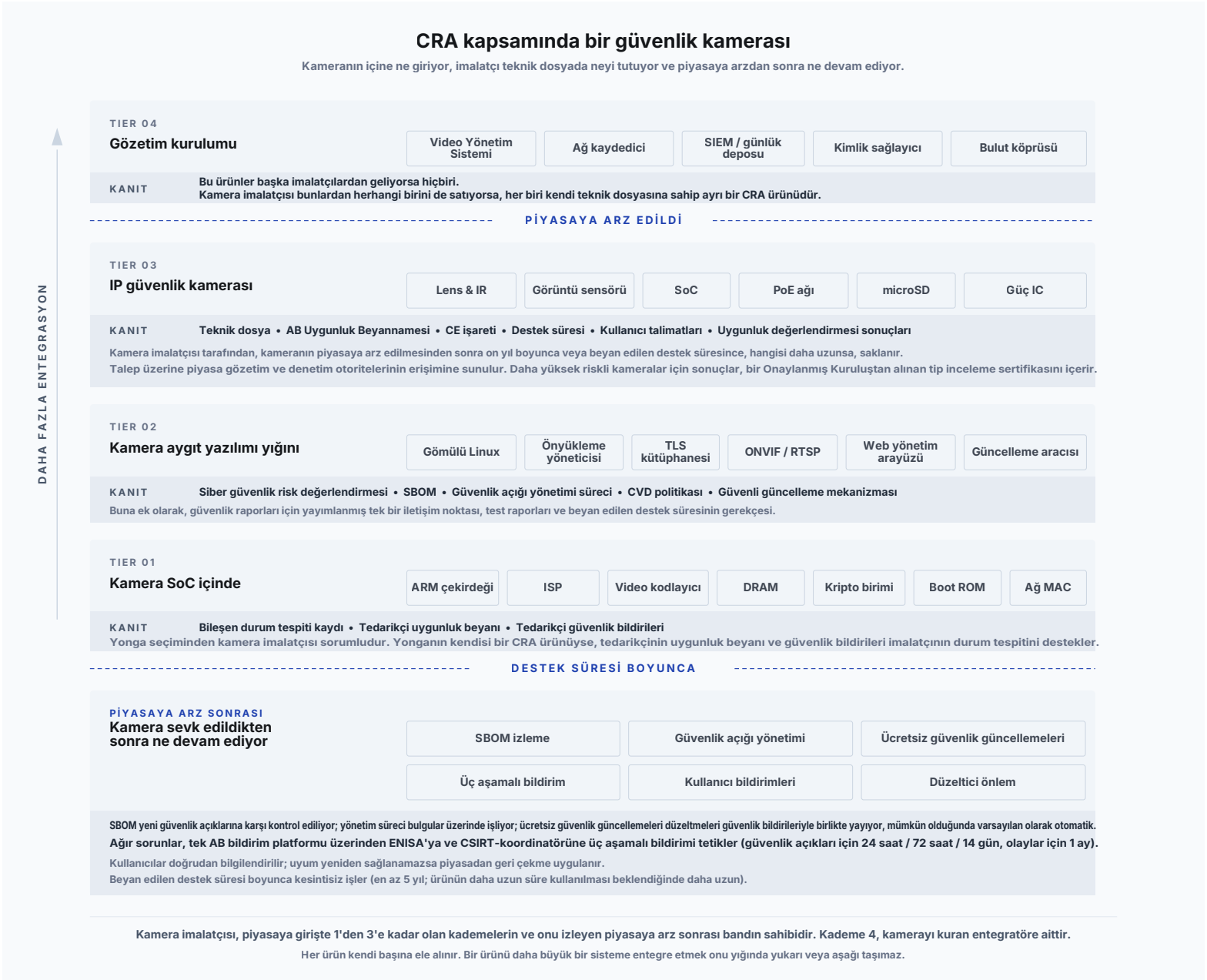
Ürün belgeleri gereklilikleri

Belgeler, ürünün piyasaya arzından sonra **en az 10 yıl** veya **tam destek süresi** boyunca, hangisi daha uzunsa o süreyle saklanmalıdır. Özet düzeyinde teknik belgeler sekiz kanıt ailesini içermelidir:

1. Genel ürün açıklaması
2. Tasarım, geliştirme ve üretim ayrıntıları (SBOM dahil)
3. Siber güvenlik risk değerlendirmesi
4. Destek süresi belirlemesi
5. Uygulanan uyumlaştırılmış standartlar ve spesifikasyonlar
6. Test raporları
7. AB Uygunluk Beyannamesi
8. Tam SBOM (piyasa gözetim ve denetim otoritelerinin talebi üzerine)

Uygunluk değerlendirmesi rotası kontrol listesi

Rotayı belirlemek için yukarıdaki sınıflandırma tablosunu kullanın. Ardından rota kararını, bunu gerekçelendiren standartlar, spesifikasyonlar, sertifikasyon şeması veya Onaylanmış Kuruluş kanıtıyla birlikte teknik dosyada saklayın.



Çalışılmış bir örnek. Aynı kademe yapısı yalnızca güvenlik kameralarına değil, her dijital unsurlu ürüne uygulanır.

Ürün güvenliği gereklilikleri

a. Piyasaya arz anında bilinen istismar edilebilir güvenlik açığı bulunmaması

Kamuya açık ve giderilmemiş istismar edilebilir güvenlik açıklarıyla ürün çıkarmayın. Bilinen bir güvenlik açığı kamu veri tabanından, tedarikçi bildiriminden, müşteri raporundan veya kendi iç takip sisteminizden gelebilir.

Bu gerekliliği karşılamak için:

- Her sürümden önce güvenlik açığı veri tabanlarını (Common Vulnerabilities and Exposures, CVE dahil) kontrol edin
- Derleme hattınızda statik ve dinamik uygulama güvenliği testleri (SAST/DAST) kullanın
- Tüm üçüncü taraf ve açık kaynak bileşenleri için bağımlılık taraması yapın
- Belirlenen her konu için risk kabulü veya azaltma kararınızı belgeleyin

b. Güvenli varsayılan yapılandırma

Ürün varsayılan hâliyle güvenli kullanılabilmelidir. Gereksiz hizmetleri kapatın, zayıf varsayılan kimlik bilgilerinden kaçının ve güvenli olmayan devreye alma modlarını kısa süreli ve kontrollü tutun. Güvenli varsayılan yapılandırma yükümlülüğü, ticari kullanıcılara yazılı sözleşmeyle sağlanan özel olarak hazırlanmış ürünler için farklı şekilde belirlenebilir; ancak ürünün başlangıç durumuna sıfırlanabilmesi her zaman korunmalıdır.

Bu gerekliliği karşılamak için:

- Varsayılan derlemelerde uzaktan erişim portlarını ve hata ayıklama arayüzlerini kapatın
- Güçlü varsayılan kimlik doğrulama mekanizmaları uygulayın
- Yönetici işlevlerini yalnızca yetkili kullanıcılarla sınırlayın
- Kullanıcı verilerini kaldırırken tüm ayarları ve gömülü yazılımı bilinen güvenli bir duruma döndüren güvenli fabrika sıfırlaması uygulayın

c. Vazgeçme seçeneğiyle otomatik güncellemeler dahil güvenlik güncellemeleri

Ürünün, devreye alındıktan sonra güvenlik sorunlarını giderebilen bir yama mekanizmasına ihtiyacı vardır. Otomatik güncellemeler uygunsa, varsayılan olarak etkinleştirin ve kullanıcılara erteleme veya vazgeçme için açık bir yol verin.

Bu gerekliliği karşılamak için:

- Güncelleme paketleri için kriptografik imzalama ve bütünlük doğrulaması uygulayın
- Geri dönüş engelleme ve güncelleme olaylarının kaydını sağlayın
- Kullanıcıları bekleyen güncellemeler konusunda uyaran bildirim sistemleri kurun
- Kullanıcıların açık bir yapılandırma arayüzü üzerinden otomatik güncellemeleri ertelemesine veya devre dışı bırakmasına izin verin

d. Yetkisiz erişime karşı koruma

Erişim kontrolleri hem yerel hem uzaktan arayüzleri korumalıdır. Amaç, yetkisiz kullanıcıların işlevlere, verilere, yapılandırmaya veya yönetim yüzeylerine ulaşmasını engellemektir.

Bu gerekliliği karşılamak için:

- Parola karmaşıklığı politikaları ve güçlü varsayılan kimlik bilgileri uygulayın
- Uygun olduğunda çok faktörlü kimlik doğrulama (MFA) kullanın
- Rol tabanlı erişim kontrolü (RBAC) ve oturum zaman aşımı uygulayın
- Başarısız erişim denemelerini kaydedin, yetkisiz faaliyeti işaretlemek için anomali tespiti kullanın ve bu olayları inceleme ve raporlama için erişilebilir kılın

e. Saklanan, aktarılan ve işlenen verinin gizliliği

Hassas verinin dururken, aktarım sırasında ve işlenirken korunması gerekir.

Bu gerekliliği karşılamak için:

- Standart şifreleme algoritmaları kullanın, örneğin dururken veri için AES-256 ve aktarım sırasında veri için TLS
- Güvenli anahtar yönetimi uygulamaları kullanın
- Gizli verileri kritik olmayan sistem bileşenlerinden ayırın
- Tüm veri erişim olayları için denetim kayıtları tutun

f. Veri, gömülü yazılım ve yapılandırma bütünlüğü

Bu gereklilik hem sistemin kendisini (gömülü yazılım, yazılım, yapılandırma dosyaları) hem de sistemin işlediği verileri (ölçümler, kontrol komutları, kullanıcı girdileri) kapsar.

Bu gerekliliği karşılamak için:

- Yalnızca güvenilir kodun çalışmasını sağlamak üzere güvenli önyükleme ve imzalı gömülü yazılım uygulayın
- Kurcalama girişimlerini tespit etmek ve raporlamak için çalışma zamanı doğrulaması kullanın
- Veri bütünlüğünü korumak için kriptografik özetler ve dijital imzalar uygulayın
- Sistem veya organizasyon sınırları arasında kriptografik anahtarları üretebilen, dağıtabilen ve doğrulayabilen altyapı kurun

g. Veri minimizasyonu

Yalnızca ürünün amaçlanan amacı için gereken verileri toplayın ve işleyin. Bu hem kişisel veriler hem teknik veriler için geçerlidir.

Bu gerekliliği karşılamak için:

- Gereksiz veri akışlarını belirlemek için mahremiyet etki değerlendirmeleri veya tasarım yoluyla veri koruma çalışmaları yürütün
- Kullanılmayan telemetriyi, tanı verilerini veya arka plan veri toplamayı kaldırın ya da isteğe bağlı hâle getirin
- Genişletilmiş veri toplamanın bağlama göre açılıp kapatılabilmesi için yapılandırılabilir veri toplama ayarları uygulayın

h. Hizmet reddi saldırıları dahil erişilebilirlik ve dayanıklılık

Olay veya saldırı sırasında temel ürün işlevleri erişilebilir kalmalı ya da kontrollü şekilde devreden çıkmalıdır.

Bu gerekliliği karşılamak için:

- Devre kesiciler, yeniden deneme mantığı, yedek mekanizmalar ve watchdog zamanlayıcıları uygulayın
- Kaynak tükenmesini önlemek için kaynak limitleri uygulayın
- Hizmet reddi senaryolarına karşı hız sınırlama ve girdi doğrulaması kullanın
- Aşırı yükleme girişimlerini engellemek için ağ düzeyi filtreleme uygulayın

i. Diğer bağlı cihazlar veya ağlar üzerinde olumsuz etki yaratmama

Ürün aynı ortamdaki diğer sistemleri aksatmamalıdır. Öngörülebilir davranmalı ve paylaşılan kaynakları aşırı kullanmaktan kaçınmalıdır.

Bu gerekliliği karşılamak için:

- Trafik şekillendirme uygulayın ve broadcast veya multicast kullanımını sınırlayın
- İletişim protokolü spesifikasyonlarına uyumu sağlayın
- Ağ taşması veya kaynak tükenmesi gibi bozucu davranışları tespit etmek ve önlemek için öz izleme kullanın

j. Dış arayüzler dahil sınırlı saldırı yüzeyi

Giriş noktalarını ve açık işlevleri en aza indirin. Buna fiziksel portlar, kablosuz arayüzler, API'ler, hata ayıklama hizmetleri ve gereksiz yazılım bileşenleri dahildir.

Bu gerekliliği karşılamak için:

- Üretim derlemelerinde kullanılmayan hizmetleri, portları ve arayüzleri kapatın
- Sistem varsayılanlarını sıkılaştırın ve kullanıcı yetkilerini sınırlayın
- Bileşenleri birbirinden izole etmek için yazılım mimarisini modülerleştirin
- Gereksiz açıklıkları belirlemek ve kaldırmak için güvenli yazılım tasarımı ilkeleri uygulayın ve tehdit modellemesi yapın

k. İstismar azaltma yoluyla olay etkisini azaltma

Bazı saldırıların başarılı olacağını varsayın. Ürün tasarımı, zararın ne kadar yayılabileceğini sınırlamalıdır.

Bu gerekliliği karşılamak için:

- Sistem bileşenlerini ayırın ve izole çalışma ortamları veya konteynerleştirme kullanarak birbirinden ayrılmış ortamlarda çalıştırın
- Kritik işlevlerin yalnızca gerekli asgari izinlerle çalışması için yetki ayrımı uygulayın
- Bir bileşenin ele geçirilmesinin saldırgana tüm sistem üzerinde kontrol vermeyeceği bir tasarım kurun

l. Kullanıcının vazgeçme seçeneğiyle güvenlikle ilgili faaliyetlerin kaydı

Erişim denemeleri ve veri değişiklikleri gibi güvenlikle ilgili faaliyetleri kaydedin. Böylece izleme ve denetim yapılabilir. CRA'nın gerektirdiği yerde kullanıcılara vazgeçme mekanizması gerekir.

Bu gerekliliği karşılamak için:

- Yapılandırılmış kayıt uygulayın, örneğin zaman damgalı JSON kayıtları
- Kayıt döndürme ve uzaktan kayıt aktarımı seçenekleriyle yerel kayıt saklama sağlayın
- Oturum açma denemeleri, yapılandırma değişiklikleri ve yazılım güncellemeleri gibi olayları anomali açısından izleyin
- İzin verilen durumlarda kaydı devre dışı bırakmak için kullanıcıya açık bir mekanizma sunun

m. Güvenli ve kalıcı veri silme ile taşınabilirlik

Kullanıcıların veri ve ayarları kalıcı olarak kaldırabilmesi için pratik bir yola ihtiyacı vardır. Veri başka bir ürün veya sisteme aktarılabiliyorsa, aktarım güvenli olmalıdır.

Bu gerekliliği karşılamak için:

- Depolama bölgelerini üzerine yazarak veya anahtarları kriptografik olarak silerek çalışan güvenli silme işlevi uygulayın
- Aktarım sırasında açığa çıkmayı önlemek için veri taşınabilirliği aktarımlarında kimliği doğrulanmış ve şifreli kanallar kullanın

Güvenlik açığı yönetimi gereklilikleri

1. Güvenlik açıklarını belirleme ve belgeleme

Üründe hangi yazılım bileşenlerinin bulunduğunu ve hangi bilinen güvenlik açıklarının bunları etkilediğini bilmeniz gerekir. SBOM (yazılım bileşen listesi), bu makine tarafından okunabilir envanteri sağlar.

Bu gerekliliği karşılamak için:

- SBOM üretimini doğrudan CI/CD hattınıza entegre edin, böylece her derleme güncel bir bileşen envanteri üretir
- Birlikte çalışabilirlik için CycloneDX, SPDX veya SWID gibi yerleşik formatları kullanın
- CVE listeleri ile CISA KEV ve ENISA EUVD gibi veri tabanlarına karşı otomatik güvenlik açığı taraması çalıştırın
- SBOM'u destek süresi boyunca teknik dosyanızın parçası olarak tutun ve talep üzerine piyasa gözetim ve denetim otoritelerine sağlayın

2. Risk yönetimi ve zamanında güvenlik güncellemeleri

Güvenlik açıkları bulunduğunda hızlıca giderin ve güvenlik güncellemelerini ulaştırın. Mümkün olduğunda güvenlik yamalarını özellik güncellemelerinden ayırın ki kritik düzeltmeler hızla kurulabilsin.

Bu gerekliliği karşılamak için:

- Güvenlik düzeltmelerinin tam sistem güncellemesi gerektirmeden dağıtılabilmesi için güncelleme mekanizmanızı tasarlayın
- Kritik bileşenlerin bağımsız yamalanabilmesi için yazılım ve gömülü yazılım yapısını düzenleyin
- Güncellemeleri bütünlük kontrolleriyle güvenli kanallar üzerinden ulaştırın
- İzlenebilirliği desteklemek ve uyumu göstermek için güncelleme faaliyetlerinin kaydını tutun

3. Düzenli güvenlik testleri

Güvenlik testi tek seferlik bir çalışma değildir. Tehditler, bağımlılıklar ve ürün davranışı değiştikçe ürünleri yaşam döngüsü boyunca test edin. Test türünü ve sıklığını risk değerlendirmesi belirlemelidir.

Bu gerekliliği karşılamak için:

- Gerçek dünya saldırılarını simüle etmek için penetrasyon testi yapın
- Güvenlik zayıflıklarını belirlemek için statik ve dinamik kod analizi uygulayın
- Girdi işleme kusurlarını ortaya çıkarmak için fuzz testi kullanın
- Özellikle önemli tasarım veya özellik değişikliklerinden sonra güvenlik kod incelemelerini ve mimari incelemeleri resmî olarak planlayıp belgeleyin

4. Güvenlik açığı alımı, CVD politikası ve duyurular

Bu gereklilik güvenlik açığı alımını, koordineli açıklamayı ve duyuru görevlerini (yukarıdaki özetin 4, 5 ve 6. maddelerini) kapsar; pratikte tek bir iş akışı olarak yürür.

CRA, güvenlik açıklarıyla ilgili iletişiminizin nasıl olacağına dair üç ayrı gereklilik adlandırır: insanların sorun bildirmesi için bir yol, koordineli açıklama politikası ve bir düzeltme yayımladığınızda bir duyuru. Her görevin ne istediği şu şekildedir.

Alım

Bildirim yapanlara açık, sürtünmesiz bir giriş yolu verin. Güvenlik açığı bildirimi için görünür bir iletişim yöntemi yayımlayın (özel e-posta veya web formu). Güvenli iletişimi destekleyin, örneğin PGP anahtarı yayımlayın. Yükümlülük, hem kendi ürününüz hem de içerdiği üçüncü taraf bileşenlerle ilgili bildirimleri kapsar.

Sınıflandırma

Her bildirimi onaylayın, bir takip sistemine kaydedin, inceleme için atayın ve tanımlı sürelerde çözün. Bildirim yapana teyit ve durum güncellemeleri gönderin. Konu üçüncü taraf bir bileşendeyse, kendi gidermenizle paralel olarak üst akış sürdürücüye yönlendirin.

Koordineli güvenlik açığı açıklama politikası

Bildirim yapanlar ve ortaklar için beklenti belirleyen bir CVD politikası yayımlayın: iletişim yöntemi, beklenen yanıt süreleri, neye taahhüt ettiğiniz, onlardan ne istediğiniz. Bildirim yapanın katkısını tanırken kullanıcıları korumak için açıklamayı koordine edin.

Düzeltme üzerine duyurular

Bir düzeltme mevcut olduğunda, çözülen konu için bir duyuru yayımlayın. CVE kimliği, etkilenen ürün sürümleri, standart bir ciddiyet derecesi (örneğin CVSS) ve kullanıcıların ne yapması gerektiğine dair açık, erişilebilir bilgi ekleyin. Hem teknik yöneticilerin hem teknik olmayan kullanıcıların anlayabileceği dilde yazın.

Geciktirilmiş kamu açıklaması

Anında açıklamanın siber güvenlik risklerinin faydalardan daha ağır bastığına dair haklı bir nedeniniz varsa ve yalnızca kullanıcıların düzeltmeyi uygulama fırsatı olana kadar, kamu açıklamasını geciktirebilirsiniz. Gerekçeyi belgeleyin.

5. Güvenli güncelleme dağıtım mekanizmaları

Güncelleme mekanizması güvenilir olmalı ve kurcalamaya dayanmalıdır. Otomatik güncellemeler teknik olarak mümkün olduğunda kullanıcıların açıkta kaldığı süreyi azaltır.

Bu gerekliliği karşılamak için:

- Güncellemeleri güvenli kanallar üzerinden aktarın ve dijital imzalarla doğrulayın
- Güncellemeleri eksik veya bozuk kurulumları önleyecek şekilde uygulayın
- Kesintiyi azaltmak ve düzeltmeleri sistemlere daha hızlı ulaştırmak için diferansiyel veya modüler güncellemeler kullanın
- Kullanıcıların veya yöneticilerin güncelleme durumunu doğrulayabilmesi için güncelleme kayıtları tutun

6. Danışma mesajlarıyla ücretsiz güvenlik güncellemeleri

Güvenlik güncellemelerini hızla ve ek ücret almadan ulaştırın; ticari kullanıcılara özel olarak hazırlanan ürünler için ayrı bir anlaşma varsa istisnadır. Her güncellemenin, kullanıcılara neyin değiştiğini ve ne yapmaları gerektiğini söyleyen açık bir danışma mesajı olmalıdır.

Bu gerekliliği karşılamak için:

- Ürün bağlamına göre kullanıcıları doğrudan bilgilendirebilen veya güncellemeleri otomatik uygulayabilen bir dağıtım sistemi kurun
- Danışma mesajlarını hem teknik hem teknik olmayan kullanıcıların anlayacağı dille yazın
- Uygun olduğunda danışma mesajlarına ciddiyet bilgisini ekleyin
- Kullanıcılara hangi aksiyonu alacaklarını söyleyin: güncellemeyi uygulamak, yapılandırmayı değiştirmek veya tehlike belirtilerini izlemek
- Düzeltme zaten mevcutken kullanıcılar açıkta kalmasın diye güvenlik güncellemelerini hazır olur olmaz gecikmeden dağıtın
- Duyuruları imalatçı kontrolündeki bir kanaldan yayımlayın ve ürünün destek sayfasından bağlayın

Ücretsiz olma ve gecikmeden dağıtma görevleri ilan edilen destek süresi boyunca işler. Özel olarak hazırlanmış ürün istisnası yalnızca ticari esası değiştirir; danışma mesajları yine uygulanır.

Teknik dosyada bulunması gerekenler

Teknik belgeler

Teknik belgeler, CRA uyumunun merkezi kanıtıdır. Temel siber güvenlik gerekliliklerini karşılamak için kullanılan tasarım, teknik ve prosedürel önlemleri kapsamalıdır. **Piyasaya arzdan önce** mevcut olmalı ve **destek süresi** boyunca güncel kalmalıdır.

Mühendislik iş akışında teknik dosya kanıtları

Adım 1	**Kapsamı belirle ve sınıflandır**	Ürün amacı, amaçlanan kullanım, piyasaya arz kararı, ürün sınıfı, standart rotası.
Adım 2	**Mimari ve risk**	Mimari, veri bağlantıları, kullanım koşulları, risk değerlendirmesi, azaltıcı önlemler.
Adım 3	**Bileşenler ve SBOM**	Makine tarafından okunabilir SBOM, üçüncü taraf bileşenler, tedarikçi girdileri, güvenlik açığı takibi.
Adım 4	**Derleme, test, güncelleme**	Güvenli varsayılanlar, sıkılaştırma, test raporları, güvenli güncelleme mekanizması, danışma mesajları.
Adım 5	**Sürüm ve destek**	Kullanıcı talimatları, AB beyannamesi, CE kanıtı, destek süresi gerekçesi, güncelleme kayıtları.

Teknik dosyanın sekiz gerekli bileşeni vardır. Birlikte **ürünün ne olduğunu**, **nasıl üretildiğini ve test edildiğini**, **hangi risklerin dikkate alındığını**, **hangi standartların uygulandığını** ve **pazarda nasıl destekleneceğini** açıklarlar. Yasal başlıkları kopyalamak zorunda değilsiniz, ancak her konunun kapsanması gerekir.

No.	Bileşen	İçermesi gerekenler
1	Genel ürün açıklaması	Amaçlanan kullanım ve işlevler, ilgili yazılım sürümleri, fotoğraflar veya çizimler (donanım için), kullanıcı bilgileri ve talimatları
2	Tasarım, geliştirme ve üretim ayrıntıları	Mimari açıklaması (bileşenler ve etkileşimler), yazılım bileşen listesi (SBOM), güvenlik açığı yönetimi süreçleri (CVD politikası, iletişim noktası, güvenli güncelleme mekanizmaları), doğrulama dahil üretim ve izleme süreçleri
3	Siber güvenlik risk değerlendirmesi	Belgelenmiş ürün risk analizi, her temel siber güvenlik gerekliliğinin ürüne nasıl uygulandığının açıklaması, belirlenen risklerin azaltılması
4	Destek süresi belirlemesi	Destek süresini belirlemek için kullanılan faktörlerin belgelendirilmesi: kullanıcı beklentileri, karşılaştırılabilir ürünler ve yasal rehberlik
5	Uygulanan uyumlaştırılmış standartlar ve spesifikasyonlar	Uygulanan uyumlaştırılmış standartların, ortak spesifikasyonların veya AB sertifikasyon şemalarının listesi; tamamen mi kısmen mi uygulandığının belirtilmesi; standartlar uygulanmadığında alternatif çözümler
6	Test raporları	Hem ürün hem güvenlik açığı yönetimi süreçleri için uygunluk kanıtı
7	AB Uygunluk Beyannamesi	Teknik dosyayı CE işareti yükümlülüklerine bağlayan beyanname kopyası
8	Tam SBOM (talep üzerine)	Piyasa gözetim ve denetim otoriteleri uyumu doğrulamak için tam SBOM isteyebilir

Tek bir konsolide teknik dosya CRA'yı ve diğer uygulanabilir AB mevzuatını (örneğin Telsiz Ekipmanları Direktifi veya ESPR) kapsayabilir; bunun için tüm uygulanabilir yükümlülüklerin dosyada yer alması gerekir.

AB Uygunluk Beyannamesi

AB Uygunluk Beyannamesi, imalatçının ürünün uygulanabilir CRA siber güvenlik gerekliliklerini karşıladığına ilişkin resmî beyanıdır. Her beyanname şunları içermelidir:

- Ürün adı, tipi ve benzersiz tanımlayıcıları
- İmalatçının adı ve adresi veya yetkili temsilci
- Sağlayıcının münhasır sorumluluğuna ilişkin beyan
- İzlenebilirliği sağlayan ürün açıklaması (isteğe bağlı görselle)
- İlgili Birlik mevzuatına uygunluğa ilişkin açık beyan
- Kullanılan uyumlaştırılmış standartlara, spesifikasyonlara veya sertifikasyonlara referanslar
- Dahil olan Onaylanmış Kuruluşun ayrıntıları (ad, numara, prosedür, sertifika numarası)
- İmza bloğu: yer, tarih, ad, görev ve imzalayanın imzası

İmzalandığında beyanname hukuken bağlayıcıdır ve imalatçının siber güvenlik uyumuna ilişkin tam sorumluluğunu teyit eder.

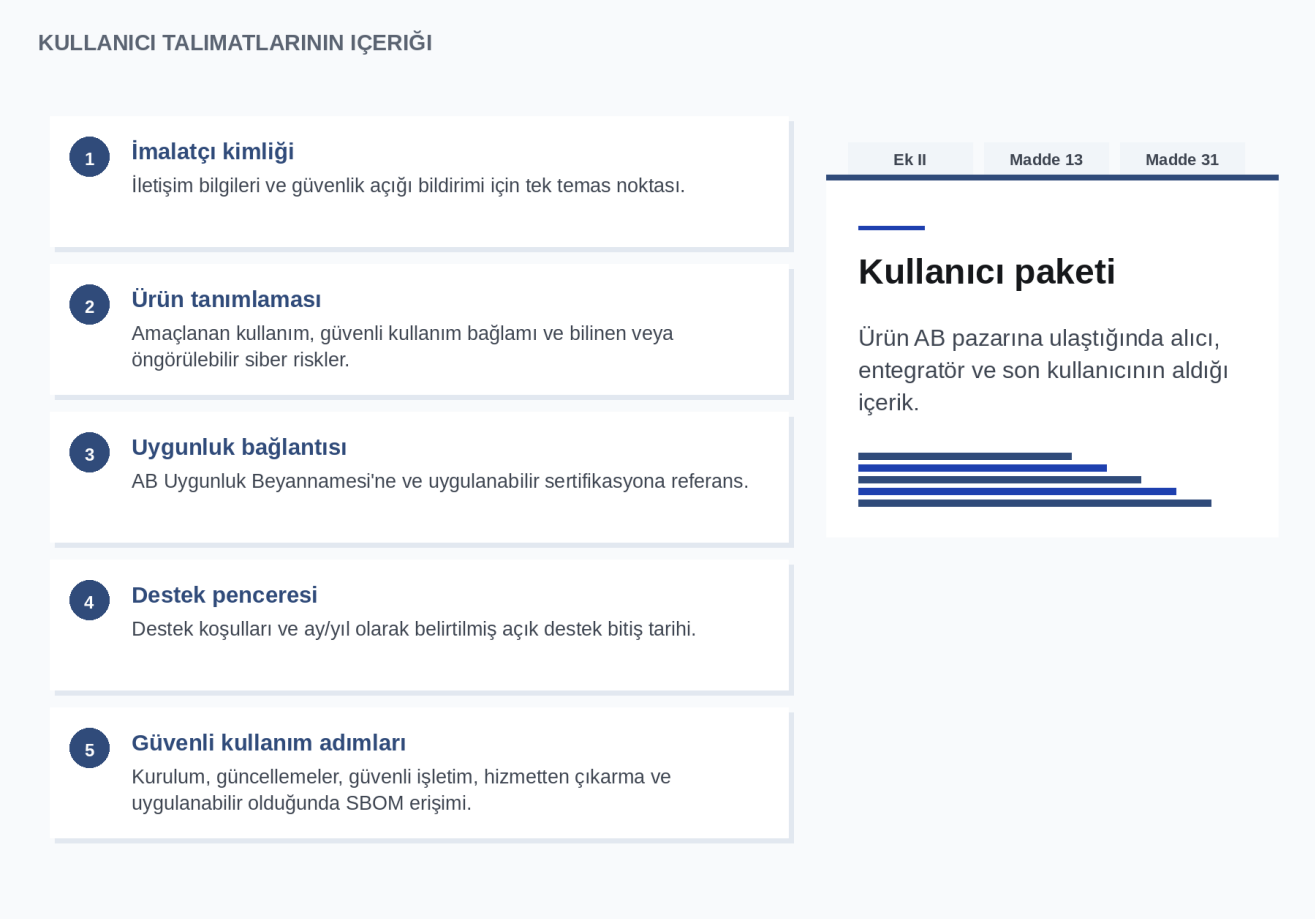
Ambalajda veya kılavuzlarda kullanılmak üzere basitleştirilmiş beyannameye izin verilir. Biçimi şöyledir: "İşbu belge ile [imalatçı], [tip/tanım] ürününün AB Tüzüğü 2024/2847'ye uygun olduğunu beyan eder. AB Uygunluk Beyannamesi'nin tam metnine şu adresten erişilebilir: [web adresi]." Bu basitleştirilmiş biçim şeffaflığı korurken evrak yükünü azaltır ve özellikle küçük imalatçılar veya çok ürünlü portföyler için yararlıdır.

Kullanıcı bilgileri ve talimatları

Kullanıcı bilgileri ve talimatları, hukuka uygun piyasaya arzın koşuludur. İmalatçılar talimatları **en az 10 yıl** veya **tam destek süresi** boyunca erişilebilir tutmalıdır. İthalatçı ve dağıtıcıların ürünü piyasaya arz etmeden veya tedarik etmeden önce talimatların mevcut, güncel ve doğru AB dilinde sağlandığını kontrol etmesi gerekir.

Kullanıcı talimatları şu içeriği gerektirir:

- İmalatçının kimliği ve iletişim bilgileri
- Güvenlik açığı bildirimi için tek temas noktası
- Ürün tanımlaması, amaçlanan kullanım ve güvenli kullanım bağlamı
- Bilinen veya öngörülebilir siber riskler
- AB Uygunluk Beyannamesi bağlantısı
- Destek koşulları ve açık destek bitiş tarihi
- Kurulum, güncellemeler, güvenli kullanım, hizmetten çıkarma ve uygulanabilir olduğunda entegrasyon ile SBOM erişimi için adım adım güvenlik talimatları



Doğru uygunluk değerlendirmesi rotasını seçme

Modül A: öz değerlendirme

Modül A (İç Kontrol), ürününüzün temel siber güvenlik gerekliliklerine uyduğunu kendi kendinize beyan etmenize olanak tanır; ürünün tasarımından ve üretiminden tam sorumluluk alırsınız. Bu rota varsayılan (sınıflandırılmamış) ürünlerin imalatçıları için kullanılabilir. Önemli Sınıf I ürünlerde yalnızca ilgili uyumlaştırılmış standartlar, ortak spesifikasyonlar veya Avrupa siber güvenlik sertifikasyon şemaları mevcutsa ve CRA rota kurallarının gerektirdiği şekilde uygulanıyorsa kullanılabilir.

Modül A kapsamında şunları yapmanız gerekir:

- Kapsamlı teknik belgeleri hazırlamak
- Ürünün tasarımını, üretim süreçlerini, siber güvenlik mekanizmalarını ve güvenlik açığı yönetimi prosedürlerini ayrıntılandırmak
- Ürünün yaşam döngüsü boyunca sürekli uyuma ilişkin sorumluluğu sürdürmek
- Ürünün operasyonel ömrü boyunca güvenlik güncellemeleri ve güvenlik açığı yönetimi için plan uygulamak
- Kayıtları en az 10 yıl erişilebilir tutmak

Modül B ve C: ürün odaklı değerlendirme

Modül B ve C, belirli bir ürün tipi için üçüncü taraf doğrulamasının gerektiği hallerde uygulanır. İmalatçının ilgili uyumlaştırılmış standartları, ortak spesifikasyonları veya sertifikasyon şemalarını uygulamadığı, yalnızca kısmen uyguladığı ya da uygulayamadığı Önemli Sınıf I ürünler için geçerlidir. Önemli Sınıf II ürünlerde imalatçı Modül B+C, Modül H veya en az "substantial" güvence düzeyinde uygulanabilir Avrupa siber güvenlik sertifikasyon şeması kullanmalıdır.

Modül B (AB tip incelemesi): Onaylanmış Kuruluş temsili bir ürün örneğini ve ilgili teknik belgeleri inceler. Tüm temel siber güvenlik gerekliliklerine uyumu doğrular ve ürün tasarımı CRA ölçütlerini karşıladığında AB tip inceleme sertifikası düzenler.

Modül C (tipe uygunluk, üretim kontrolü): İmalatçı tüm üretim birimlerinin Modül B kapsamında sertifikalandırılmış onaylı tipe uygun olmasını sağlar. İmalatçı CE işaretini iliştirir, AB Uygunluk Beyannamesi'ni düzenler ve kayıtları en az 10 yıl erişilebilir tutar. Modül B ve C birlikte belirli bir ürün modelinin teknik olarak uyumlu olduğunu ve her üretim partisinin onaylı tasarımla tutarlı kaldığını gösterir.

Modül H: süreç odaklı değerlendirme (tam kalite güvencesi)

Modül H (Tam Kalite Güvencesi), tekil ürün testinden çok imalatçının tüm iç kalite sistemine odaklanır. Önemli Sınıf I ve Sınıf II ürünler için kullanılabilir. Kritik ürünler, ilgili koşullar karşılandığında sertifikasyon rotasını kullanır; koşullar karşılanmadığında Önemli Sınıf II ürünler için mevcut olan aynı rotaları kullanır.

Modül H kapsamında şunları yapmanız gerekir:

- Tüm ürün kategorisi için tasarım, geliştirme, üretim, test ve güvenlik açığı yönetimini kapsayan kalite sistemi kurmak ve sürdürmek
- Kalite sistemini değerlendirme ve onay için Onaylanmış Kuruluşa sunmak

- Sürekli uyumu doğrulamak için Onaylanmış Kuruluşun devam eden gözetimini (denetimler, incelemeler ve süreç gözden geçirmeleri) kabul etmek

Onaydan sonra, her ürün tipi için Onaylanmış Kuruluş incelemesini tekrarlamadan bu kalite sistemi altında üretilen tüm ürünler için uygunluk beyannamesi düzenleyebilirsiniz.

Rotalar arasındaki temel fark:

- Modül B+C: ürüne odaklanır. Temsili bir ürün tipi test edilir ve sertifikalandırılır.
- Modül H: sürece odaklanır. İmalatçının tüm tasarım ve üretim sistemi sertifikalandırılır ve izlenir.

CRA'nın daha geniş AB mevzuat çerçevesindeki yeri

CRA tek başına durmaz. Bir imalatçı için pratik soru şudur: CRA çalışmam başka bir AB rejimi altında nereden tasarruf sağlar ve nerede paralel yürütülecek ayrı yükümlülükler kalır?

CRA çalışmanızın yeniden kullanılabileceği yerler

- **Yüksek riskli yapay zekâ sistemleri (Yapay Zekâ Yasası, Tüzük 2024/1689).** Ürününüz CRA kapsamındaki yüksek riskli bir yapay zekâ sistemiyse, CRA temel siber güvenlik gerekliliklerini karşılamak, AB Uygunluk Beyannamenizin kapsadığı ölçüde Yapay Zekâ Yasası'nın siber güvenlik gerekliliklerini de karşıladığınız sayılır. Uygunluk değerlendirme prosedürü kural olarak Yapay Zekâ Yasası rejimi üzerinden yürür, Önemli ve Kritik CRA ürünleri için bir istisna vardır. CRA siber güvenlik risk değerlendirmesi, veri zehirlenmesi ve düşmanca saldırılar gibi yapay zekâya özgü riskleri de hesaba katmalıdır.
- **Diğer Birlik mevzuatı ile konsolide risk değerlendirmesi.** CRA, ürünün her iki rejime tabi olduğu durumlarda siber güvenlik risk değerlendirmesinin başka bir Birlik mevzuatı tarafından gerekli kılınan daha geniş bir risk değerlendirmesinin parçasını oluşturmasına açıkça izin verir. Tek bir değerlendirme çıktısı, iki düzenleyici kullanım.
- **Rejimler arası tek teknik dosya.** Teknik dosya bölümünde belirtildiği gibi, tek bir konsolide teknik dosya CRA'yı diğer uygulanabilir Birlik mevzuatıyla birlikte kapsayabilir, her rejimin yükümlülükleri ele alındığı sürece. Aynı ürünün halihazırda Telsiz Ekipmanları Direktifi, Sürdürülebilir Ürünler İçin Eko Tasarım Tüzüğü veya diğer ürün mevzuatı kapsamında belgeye ihtiyacı varsa yararlıdır.
- **Yenileme, bakım ve onarımın ortak tanımları.** CRA bu tanımları Sürdürülebilir Ürünler İçin Eko Tasarım Tüzüğü'nden ithal eder. Bir hizmet işleminin esaslı değişiklik sayılıp sayılmadığını analiz ederken referans, CRA'ya özgü bir terim değil, Eko Tasarım tanımlarıdır.

Ayrı yükümlülüklerin kaldığı yerler

- **Yapay Zekâ Yasası'nın geri kalanı.** Siber güvenlik, Yapay Zekâ Yasası'nın yalnızca bir dilimidir. Risk sınıflandırması, şeffaflık, veri kümesi yönetişimi, insan gözetimi, yapay zekâ davranışının piyasaya arz sonrası izlenmesi ve geri kalanı, CRA'nın ele almadığı Yapay Zekâ Yasası görevleridir. CRA uyumlu siber güvenlik, genel olarak Yapay Zekâ Yasası uygunluğu varsayımı değildir.
- **Eko Tasarım ve dijital ürün pasaportu içeriği.** Eko Tasarım'ın enerji verimliliği, dayanıklılık, onarılabilirlik puanlaması ve dijital ürün pasaportunun sürdürülebilirlik içeriği hakkındaki gereklilikleri CRA kapsamı değildir. CRA kanıt zinciri Eko Tasarım çalışmasının yanında yer alabilir ancak onun yerini almaz.
- **Veri Yasası'nın IoT veri erişim hakları.** Veri Yasası, kullanıcılara bağlantılı ürünlerinin ürettiği veriye erişim, paylaşım ve aktarım için sözleşmeden doğan haklar verir. CRA bu verinin güvenliğini kapsar; erişim hakları rejimini düzenlemez. Farklı yükümlülük, farklı kanıt.
- **Hatalı ürünler için ürün sorumluluğu.** Ürün Sorumluluğu Direktifi (2024/2853), hatalı ürünlerin sebep olduğu zararlar için imalatçıya kusursuz sorumluluk yükler. CRA, piyasaya arz sonrası güvenlik güncellemelerinin eksikliğinin sorumluluğu tetikleyen kusur olabileceğine işaret eder. Sözleşmelerinizin, sigortanızın ve olay senaryolarınızın bu maruziyeti CRA uygunluğundan bağımsız olarak hesaba katması gerekir.

CRA Evidence nasıl yardımcı olur

CRA Evidence, AB Siber Dayanıklılık Tüzüğü yükümlülüklerini doğrulanabilir ürün kanıtına dönüştürür; uyum platformunu teknik danışmanlıkla birleştirir.

Platform

CRA hazırlığının arkasındaki kanıtı yönetmek için tek yer:

- **SBOM ve bileşen envanteri:** ürün sürümleri ve release'ler için CycloneDX, SPDX ve HBOM kayıtları
- **CI/CD kanıt otomasyonu:** taramalar, SBOM yüklemeleri, release kapıları ve denetim kayıtları için CLI ve API iş akışları
- **İmzalı SBOM ve köken:** sürümlenmiş kanıt, tedarikçi beyanları ve özen kayıtları
- **Güvenlik açığı operasyonları:** CISA KEV, EPSS, VEX, izleme, triyaj ve bildirim iş akışları
- **Teknik dosya ve CE kanıtı:** AB beyan kayıtları, saklama geçmişi ve QR bağlantılı ürün uyum pasaportları

Teknik danışmanlık

CRA yükümlülüklerini ürün, mimari, release süreci ve tedarikçi modeli için mühendislik kararlarına çevirmeye odaklı destek.

- **Teknik Hazırlık Sprinti:** temel gereklilik boşluk incelemesi, mimari öneriler ve önceliklendirilmiş aksiyon planı
- **CRA Program Liderliği:** sorumluluk modeli, yükümlülük takibi, kanıt kilometre taşları ve teknik dosya bakımı
- **Yetkili Makam ve Olay Müdahale Planı:** bildirim iş akışları, soru playbook'ları, kullanıcı iletişimi ve kanıt paketi hazırlığı
- **Mevzuat uyumu eşleştirmesi:** CRA kanıtını Data Act, ESPR, AI Act, RED ve sektörel gerekliliklerle bağlama
- **Teknik atölyeler:** ürün, geliştirme, güvenlik, uyum ve tedarikçi ekipleriyle uzaktan veya yerinde oturumlar

Araçtan bağımsız: CRA Evidence CycloneDX, SPDX, Grype, Trivy, CI/CD hatları ve konu takip sistemleriyle entegre olur.

Pratik ilk adım

Bir ürün ailesi seçin. Sahibini, kapsam kararını, SBOM'u, güvenlik açığı iş akışını, teknik dosya boşluklarını ve release kanıtını eşleyin. Bu, uyumu ayrı bir projeye çevirmeden ekibe somut bir CRA başlangıç noktası verir.

Ürününüz için CRA Evidence kapsamını craevidence.com/tr adresinde inceleyin. Ücretsiz 45 dakikalık değerlendirme için craevidence.com/tr/assessment adresinden randevu alın.

Bu rehber CRA Evidence tarafından hazırlanmıştır ve AB Tüzüğü 2024/2847 esas alınmıştır. Bilgilendirme amaçlıdır ve hukuki danışmanlık değildir.