TÜRKİYE'NİN MAKİNECİLERİ
"Dünya Bizimle Çalışıyor"

Aralık 2025

AB Siber Dayanıklılık Yasası:
Tarım Makineleri Açısından İncelenmesi ve Uygulama Kılavuzu

AB Siber Dayanıklılık Yasası Nedir?

Avrupa Birliği Siber Dayanıklılık Yasası (Cyber Resilience Act – CRA), en basit haliyle, dijital bileşen içeren ürünlerin siber açıdan güvenli olmasını zorunlu kılan bir düzenlemedir.

Siber Dayanıklılık Yasası'nın ana hedefi, ürün kaynaklı siber güvenlik risklerini azaltmak ve bu riskleri daha ürün piyasaya çıkmadan önce kontrol altına almaktır. Yasa, siber güvenliği bir "sonradan eklenen özellik" olmaktan çıkarıp, ürünün doğal bir parçası haline getirmeyi amaçlar.

Avrupa Birliği bu yasa ile net bir duruş sergileyerek siber güvenliği yalnızca kullanıcıya bırakmamaktadır. Güvenlik meselesi artık üreticinin temel yükümlülüklerinden birisi haline getirilmektedir.

AB Siber Dayanıklılık Yasasının Kapsamı Nedir?

Siber Dayanıklılık Yasası'nın kapsamı oldukça geniştir. Yasa, "dijital unsurlar içeren ürünler" (Product with Digital Elements – PDE) kavramını esas alır. Bu kavram, günlük hayatta kullanılan pek çok ürünü içine alır.

Bir ürün:

- içinde yazılım barındırıyorsa,
- yazılım sayesinde çalışıyorsa,
- veri alıyor, işliyor veya iletiyorsa,
- başka cihazlara ya da ağlara bağlanabiliyorsa

Siber Dayanıklılık Yasası kapsamına girer. Bu noktada ürünün tarımda, sanayide, evde, kamu alanında kullanılıyor olması fark etmez.

Siber Dayanıklılık Yasası özellikle şu tür riskleri hedef almaktadır;

- Ürünlerin varsayılan olarak güvensiz gelmesi
- Kolay tahmin edilebilir veya hiç olmayan şifreler
- Güncellenemeyen yazılımlar
- Uzun yıllar desteklenmeyen dijital sistemler
- Güvenlik açığı ortaya çıktığında sessiz kalınması

Ceyhun Atuf Kansu Cad. No: 120
PK 06520 Balgat - Ankara - TR
Telefon: +90 312 447 27 40
Faks: +90 312 446 96 05

www.makinebirlik.com
www.turkishmachinery.org
www.turkiyeninmakinecileri.org

Aşağıdaki noktalar AB Siber Dayanıklılık Yasası'nı özetler niteliktedir;

Ürünlerde zorunlu asgari siber güvenlik

1. **Siber Dayanıklılık Yasası, "ürün güvenliği" anlayışını siber boyuta genişletir.** Buna göre üreticilerin:

    - Güvenlik risk analizi yapması,
    - Güvenli tasarım ve geliştirme süreçleri uygulaması,
    - Varsayılan olarak güvenli yapılandırmalar sunması,
    - Zayıf şifreler gibi riskli uygulamaları engellemesi zorunlu hale gelmektedir.

2. **Güvenlik açıklarının bildirilmesi (24 saat)**

    - Üreticiler, kritik güvenlik açıklarını tespit ettiklerinde 24 saat içinde AB Siber Güvenlik Birimi'ne (ENISA üzerinden CSIRTs) bildirmek zorundadır.

3. **Ürün yaşam döngüsü boyunca destek verilmelidir**.

    - Piyasaya sürülen bir ürün için üretici:
        - En az birkaç yıl boyunca güvenlik güncellemeleri sunmak,
        - Yamanın çıkarılmasından sonra onu hızlı ve risksiz şekilde uygulanabilir kılmak zorundadır.

4. **Ürün kategorileri ve risk sınıfları:**

    - Siber Dayanıklılık Yasası, farklı risk seviyelerine sahip ürün kategorileri tanımlar. Yüksek riskli kategoriler (ör. ağ cihazları, kimlik doğrulama sistemleri, kritik altyapı bileşenleri) daha sıkı doğrulama ve sertifikasyon süreçlerinden geçer.

5. **CE işareti artık siber güvenliği de kapsamaktadır.**

    Bir ürünün AB'de satılabilmesi için gerekli olan CE uygunluk işareti, artık ürünün CRA gereklerini karşılamasını da içermektedir. Yani üretici:

    - Ürününü güvenlik testlerinden geçirip
    - Uygunluk beyanı hazırlamadan piyasaya süremez.

6. **Etki alanı genişledi.**

    - Yasa sadece AB içi üreticileri değil, AB pazarına ürün satan tüm küresel üreticileri kapsamaktadır. Ayrıca üçüncü taraf yazılım bileşenleri ve açık kaynak kullanımı için de özel yükümlülükler bulunur (özellikle tedarik zincirinin güvenliği açısından).

TÜRKİYE'NİN MAKİNECİLERİ
"Dünya Bizimle Çalışıyor"

AB Siber Dayanıklılık Yasası Tarım Makineleri Açısından Neden Önemlidir?

Halihazırda üretilen tarım makinelerinin çok önemli bir kısmı geniş sayıda dijital bileşen, sensör, telemetri, IoT/uzaktan kontrol sistemi içerdiği için Siber Dayanıklılık Yasası kapsamına girmektedir. Siber Dayanıklılık Yasası'nın istisnası kapsamında belirli sektörler yoksa (ör. otomotiv, tıbbi cihazlar gibi özel rejimlerde olabilir) tarım makineleri için ayrı bir muafiyet bulunmamaktadır.

Avrupa Tarım Makineleri Endüstrisi Derneği (CEMA) tarafından yayınlanan Siber Dayanıklılık Yasası Uygulama Kılavuzu tarım makineleri sektörünün bakış açısından Siber Dayanıklılık Yasası'nın kapsamlı bir yorumunu sunmaktadır.

CEMA tarafından hazırlanan bu uygulama kılavuzunun amacı tarım makinesi üreticilerine AB Siber Dayanıklılık Yasası'nı (CRA 2024/2847) doğru yorumlayıp uygulamaları için sektör-özel rehberlik sağlamaktır. Bu metin yasal yorum yerine sektörün uygulama rehberidir ve bağlayıcı değildir.

1. **KAPSAM**

   Dokümanın en geniş bölümü Siber Dayanıklılık Yasası (CRA)'nın tarım makinelerine nasıl uygulanacağını açıklar. Bir tarım makinesi aşağıdaki örnekler gibi doğrudan veya dolaylı veri bağlantısı oluşturabilecek herhangi bir fiziksel veya mantıksal arabirim içeriyorsa CRA kapsamındadır. Örnekler dokümanın 3–4. sayfalarında belirtilmiştir.

   - USB portu
   - OBD portu
   - GPS bağlantısı
   - Bluetooth / radyo bağlantısı
   - JTAG/Debug portu

   Kapsam dışında kalan makineler:

   - Hiçbir veri bağlantısı olmayan makineler
   - Tamamen mekanik makineler

   Siber Dayanıklılık Yasası (CRA), ancak başka bir AB düzenlemesi aynı veya daha yüksek güvenlik seviyesi sağlıyorsa devre dışı kalabilir. **Tarım makineleri için böyle bir istisna yoktur; dolayısıyla CRA her durumda uygulanır.**

   Siber Dayanıklılık Yasası (CRA), **"aynı özelliklere sahip, birebir aynı" (identical) yedek parçaları kapsam dışında bırakır.** Ancak bir parçada değişiklik varsa (ör. donanım eskidiği için alternatif kullanılması) üretici bunun "önemli değişiklik" olup olmadığını analiz etmeli ve teknik dosyayı güncellemelidir.

Ceyhun Atuf Kansu Cad. No: 120
PK 06520 Balgat - Ankara - TR
Telefon: +90 312 447 27 40
Faks: +90 312 446 96 05

www.makinebirlik.com
www.turkishmachinery.org
www.turkiyeninmakinecileri.org

2. ÖNEMLİ ve KRİTİK ÜRÜNLER (Annex III & Annex IV)

Doküman, tarım makinelerinin Annex III (Important) veya Annex IV (Critical) kategorilerine genelde girmediğini açıklar. Bu listeler daha çok **güvenlik çipleri, güvenli mikrodenetleyiciler, yüksek güvenlik seviyesi gerektiren ICT ürünleri** içindir. Tarım makinası bu tür bileşenleri içerse bile makinanın kendisi otomatik olarak bu sınıfa geçmez. Sadece bileşen kendi sınıfında değerlendirilir.

3. ÖNEMLİ KAVRAM: SUBSTANTIAL MODIFICATION

Siber Dayanıklılık Yasası (CRA)'ya göre bir ürün üzerinde yapılan değişiklik yeni bir fonksiyon ekliyorsa, **güvenlik risklerini değiştiriyorsa, ürünün "intended purpose" (amaçlanan kullanım) tanımını değiştiriyorsa "önemli değişiklik/ substantial modification" olarak kabul edilir ve yeniden uygunluk değerlendirmesi gerekir.**

Her değişiklik için etki analizi (impact analysis) zorunludur.

4. OEM (ORİJİNAL EKİPMAN ÜRETİCİSİ) – TEDARİKÇİ İLİŞKİLERİ

Bu kısım Siber Dayanıklılık Yasası kapsamındaki sorumluluk paylaşımını açıklamaktadır.

OEM'in Yükümlülükleri:

- Entegre edilecek tüm bileşenlerde due diligence/ gerekli özen sağlamak zorundadır (CE işareti, güncelleme geçmişi, bilinen zafiyetler vb. kontrol edilmelidir).
- Ürünün genel siber güvenlik uyumluluğundan bileşen üreticisi değil tamamen OEM sorumludur.
- Bir bileşen zafiyeti bulunursa tedarikçiye bildirmek ve çözümlemek OEM'in görevidir. (Tedarikçi destek vermiyorsa OEM çözümü kendi sağlamak zorunda kalabilir.)

Tedarikçi'nin Yükümlülükleri:

- Bileşeni OEM'e entegre edilebilecek şekilde güvenli yapılandırma talimatlarıyla sunmak zorundadır. Ancak bileşenler secure-by-default[1] olmadan piyasaya sunulabilir; çünkü güvenli yapılandırma entegrasyon sırasında OEM tarafından yapılacaktır.

[1] *secure by default bir sistemin, ürünün ya da yazılımın ilk kurulduğu anda (ekstra ayar yapmadan) güvenli şekilde çalışacak biçimde tasarlanmış olması demektir.

Kişiye Özel Ürün İstisnası

- OEM ile tedarikçi arasındaki özel anlaşmalarla Siber Dayanıklılık Yasası'nın getirdiği bazı gerekliliklerden sapılabilir, ancak bu sadece belirli iş kullanıcıları için üretilen özelleştirilmiş ürünlerde geçerlidir.

5. BİLEŞEN TEDARİKÇİSİNİN SORUMLULUKLARI

- Bu bölüm komponent üreticileri için oldukça önemlidir.
- Bileşenler Siber Dayanıklılık Yasası kapsamında birer "product with digital element/ dijital öğeler içeren ürün" sayılır. Bu nedenle;
  - Risk değerlendirmesi
  - Talimat dokümantasyonu
  - Entegrasyon bilgileri sağlanmalıdır.
- Bileşenler "secure by default" olmadan satılabilir çünkü bu entegrasyon aşamasında sağlanacaktır. Bileşenler farklı güvenlik seviyeleri ile piyasaya sunulabilir. Bu durum tarım makinesi endüstrisinde de esneklik sağlar.

6. ZAFİYET YÖNETİMİ ve DESTEK SÜRESİ

- Siber Dayanıklılık Yasası, üreticilere **zorunlu zafiyet yönetimi** sürecini getirmektedir. Üreticinin görevleri arasında;
  - Üründe tespit ettiği **aktif olarak istismar edilen zafiyetleri ENISA (Avrupa Birliği Siber Güvenlik Ajansı)'ya bildirmek zorundadır.**
  - Ürün ömrü boyunca tüm zafiyetleri yönetmek zorundadır.
  - Dokümanda, ENISA'nın kuracağı bildirim platformunun henüz tanımlı olmadığı da belirtilmiştir.
- Siber Dayanıklılık Yasası, destek süresi olarak minimum **5 yıl** istemektedir ancak CEMA tarım makineleri için **10 yıllık destek süresi önermektedir.** Bunun gerekçesi olarak tarım makinelerinin uzun kullanım ömrü, OTA[2] güncellemelerinin sınırlı olması (yalnızca %20 civarında) ve Çoğu güncellemenin bayiler tarafından yapılması gösterilmektedir. Ayrıca güncellemelerin yayımlandıktan sonra **10 yıl boyunca indirilebilir** olması tavsiye edilmektedir.

7. BELGELENDİRME ve TEKNİK DOSYA

- Siber Dayanıklılık Yasası gereğince aşağıda sıralı örnekler gibi teknik belgeler hazırlanmalı ve güncellenmelidir. Siber Güvenlik Yasası'nda bu gerekliliklere sürekli atıf yapılmaktadır.

[2] Bir cihazın yazılımının, fiziksel müdahale olmadan, uzaktan güncellenmesidir.

- Ürün yaşam döngüsüne ilişkin risk değerlendirmesi
- SBOM (software bill of materials, yazılım içerik listesi)
- Entegrasyon talimatları
- Zafiyet yönetimi kayıtları

SONUÇ

Avrupa Birliği Siber Dayanıklılık Yasası (CRA), dijital unsurlar içeren tüm ürünlerde olduğu gibi tarım makineleri sektöründe de önemli bir paradigma değişimini beraberinde getirmektedir. Günümüzde tarım makineleri yalnızca mekanik sistemler olmaktan çıkmış; yazılım, sensörler, uzaktan bağlantı, veri analitiği ve otomasyon bileşenleriyle yüksek derecede dijitalleşmiş kompleks ürünlere dönüşmüştür. Bu dönüşüm, verimlilik ve sürdürülebilirlik açısından büyük avantajlar sağlarken, siber güvenlik risklerini de aynı ölçüde artırmaktadır.

CRA'nın temel yaklaşımı olan "secure by design" ve "secure by default" ilkeleri, tarım makineleri üreticileri için artık bir tercih değil, yasal bir zorunluluk haline gelmektedir. Ürünlerin piyasaya arz edilmeden önce siber riskler açısından değerlendirilmesi, güvenli yazılım geliştirme süreçlerinin uygulanması, zafiyet yönetimi ve düzenli güncellemelerin sağlanması gerekecektir. Bu durum, özellikle yazılım ve bağlantılı hizmetler sunan traktörler, hasat makineleri, akıllı ekim sistemleri ve uzaktan yönetilen tarım ekipmanları açısından doğrudan etki yaratacaktır.

Yasa, büyük ölçekli ve kurumsallaşmış üreticiler için mevcut uyum süreçlerinin güçlendirilmesi anlamına gelirken, KOBİ niteliğindeki tarım makinesi üreticileri için daha ciddi bir dönüşüm ihtiyacını ortaya koymaktadır. Teknik bilgi, insan kaynağı ve maliyet açısından yeni yükümlülükler doğması muhtemeldir. Ancak orta ve uzun vadede bu yükümlülüklerin, ürün kalitesini artırarak Avrupa pazarında rekabet gücünü desteklemesi beklenmektedir.

Tarım sektörünün kritik altyapı niteliği taşıması da CRA'nın önemini artırmaktadır. Siber saldırılar yalnızca makine arızalarına değil; gıda üretiminde aksamalara, veri kayıplarına ve tedarik zinciri bozulmalarına yol açabilmektedir. Bu nedenle tarım makinelerinin siber dayanıklılığının artırılması, yalnızca üreticiler için değil, gıda güvenliği ve kırsal ekonomik sürdürülebilirlik açısından da stratejik bir konudur.

Sonuç olarak, Siber Dayanıklılık Yasası tarım makineleri sektörü için kısa vadede uyum maliyetleri ve operasyonel dönüşüm gerektiren bir düzenleme olsa da, uzun vadede daha güvenli, dayanıklı ve rekabetçi ürünlerin ortaya çıkmasını teşvik edecektir. CRA'ya erken uyum sağlayan üreticiler, yalnızca yasal riskleri azaltmakla kalmayacak; aynı zamanda Avrupa pazarında güvenilir marka algısını güçlendirerek önemli bir avantaj elde edecektir.

Kaynakça

1- *TARMAKBİR, Siber Dayanıklılık Yasası Bilgi Notu*
2- *CEMA, Siber Dayanıklılık Yasası Uygulama Kılavuzu*

Ek-1: CEMA- Siber Dayanıklılık yasası Uygulama Kılavuzu

CEMA
European Agricultural Machinery Association

AB Siber Dayanıklılık Yasası (CRA 2024/2847) hakkında CEMA uygulama kılavuzu

Sürüm 1 - Aralık 2025

İçindekiler

Belgenin amaçları

Bu belge, AB Siber Dayanıklılık Yasası'nın (CRA) CEMA tarafından yorumlanmasını sağlamak, üreticiler için uygulamanın kolaylaştırılması, sektörümüzde bu uygulamanın tutarlılığının sağlanması ve CEMA'nın dışa yönelik tutumlarının oluşturulması ve standardizasyon çalışmaları için bir temel oluşturmasını amaçlamaktadır.

Bu belge, CEMA üyelerinin CRA'yı anlamasına ve uygulamasına destek olmak amacıyla hazırlanmıştır; geçerli mevzuatın yerini almaz ve herhangi bir ek gereklilik getirmez. Sunulan yorumlar yasal olarak bağlayıcı değildir ve üreticilerin CRA'ya tam uyum sağlamaktan sorumlu olduğu gerçeğini değiştirmez. Bu belge yalnızca bir yardımcı araçtır ve gerektiğinde güncellenebilir.

Konu: Kapsam

Referans CRA	**CRA 2024/2847 metni**	**CEMA yorumu**
Madde	**Kapsam**	
Madde 2 (1)	Bu Yönetmelik, **piyasada temin edilebilen dijital unsurlar içeren ürünlere** uygulanır; bu ürünlerin **amaçlanan kullanımı** veya **makul olarak öngörülebilir kullanımı**, adresine **doğrudan veya dolaylı olarak mantıksal** veya **fiziksel veri bağlantısı** veya ağ bağlantısı içermektedir. cihaz veya ağ ile doğrudan veya dolaylı mantıksal veya fiziksel veri bağlantısı içeren ürünlere uygulanır.	"Piyasada sunulan" kavramı Mavi Kılavuzda[1] 2022 §2.2'de yer almaktadır. Varsayım: Tüm tarım makineleri, piyasada sunulduğu ve CE işareti gerektirdiği için CRA'nın kapsamına girer, ancak Ek I (temel gereklilikler) yalnızca ilgili tanımlara göre yazılım, donanım ve uzaktan veri işlemeyi (varsa) içeren "Elektronik Bilgi sistemi" için geçerlidir. En azından tanımlandığı şekliyle amaçlanan kullanım veya makul olarak öngörülebilir kullanım, kullanılan teknolojiye (mantıksal veya fiziksel) bakılmaksızın, harici bir kaynaktan makineyle veri bağlantısı kurmanın bir yolunu içermelidir. Kapsamdaki ürünlere örnekler: - makine içindeki bir USB bağlantı noktası. - Makine içindeki bir ODB bağlantı noktası. - GPS bağlantısı. - Bluetooth bağlantısı. - Mikrodenetleyicinin JTAG/Hata Ayıklama bağlantı noktası (bkz. "Makul Olarak Öngörülebilir Kullanım").

[1] https://single-market-economy.ec.europa.eu/news/blue-guide-implementation-product-rules-2022-published-2022-06-29_en

		Kapsam dışı ürün örnekleri: - hiçbir veri bağlantısı olmayan makine. - tamamen mekanik bir makine.
Madde 2 (2)	Bu Tüzük, aşağıdaki Birlik yasal düzenlemelerinin uygulandığı dijital unsurlar içeren ürünlere uygulanmaz: (a) (AB) 2017/745 sayılı Tüzük; (b) (AB) 2017/746 sayılı Tüzük; (c) (AB) 2019/2144 sayılı Tüzük.	Aşağıdaki dijital unsurlar içeren ürünler hariçtir: (a) Tıbbi cihazlar (b) İn vitro tanı amaçlı tıbbi cihazlar (c) Tip Onaylı Araç Kategorisi *L, M, N, O
Madde 2 (3)	Bu Yönetmelik, (AB) 2018/1139 sayılı Yönetmelik uyarınca sertifikalandırılmış dijital unsurlar içeren ürünlere uygulanmaz.	Havacılık hariç tutulmuştur.
Madde 2 (4)	Bu Yönetmelik, Avrupa Parlamentosu ve Konseyi'nin 2014/90/AB sayılı Direktifi kapsamına giren ekipmanlara uygulanmaz.	Denizcilik hariç tutulması.
Madde 2 (5)	Bu Yönetmeliğin , Ek I'de belirtilen temel siber güvenlik gerekliliklerinin tümünü veya bir kısmını ele alan diğer Birlik kuralları kapsamındaki dijital unsurlar içeren ürünlere uygulanması, aşağıdaki durumlarda sınırlandırılabilir veya hariç tutulabilir: bu tür bir **sınırlama veya hariç tutma**, söz konusu ürünlere uygulanan genel düzenleyici çerçeve ile tutarlıdırsa; ve (a) bu sınırlama veya hariç tutma, söz konusu ürünlere uygulanan genel düzenleyici çerçeve ile tutarlıdır; ve (b) sektörel kurallar, **bu Tüzükte öngörülenle aynı veya daha yüksek bir koruma düzeyini** sağlar. Komisyon, bu sınırlama veya istisnanın gerekli olup olmadığını, ilgili ürünleri ve kuralları ve varsa sınırlamanın kapsamını belirterek, bu Tüzüğü tamamlamak üzere 61. maddeye göre delege edilmiş işlemleri kabul etme yetkisine sahiptir.	CRA, tüm türdeki siber güvenlik tehditlerini (örneğin, kullanıcının sağlığı ve güvenliği, dolandırıcılık, gizlilik, operasyonel riskler) ele almaktadır. AG sektörüne uygulanabilir başka hiçbir düzenleme CRA'nın sağladığı koruma düzeyine eşit veya daha yüksek bir koruma düzeyi sağlamadığından, CRA tüm durumlarda geçerlidir.
Madde 2 (6)	Bu Yönetmelik aşağıdakilere uygulanmaz **piyasada** temin edilebilen aynı parçaların yerine	Burada ele alınan senaryolar: 1. Araç hala üretimdedir.

	dijital elemanlar içeren ürünlerdeki bileşenler ve 'e göre değiştirilecek bileşenlerle aynı özelliklere sahiptir. [bkz. ayrıca Gerekçe (29)]: Piyasada bulunan dijital unsurlar içeren ürünlerin etkin bir şekilde onarılabilmesini ve dayanıklılıklarının artırılabilmesini sağlamak için yedek parçalar için bir muafiyet sağlanmalıdır. Bu muafiyet, hem bu Tüzüğün uygulama tarihinden önce piyasaya sunulan eski ürünlerin onarılması amacıyla kullanılan yedek parçaları hem de bu Tüzüğe göre uygunluk değerlendirme prosedüründen geçmiş yedek parçaları kapsamalıdır.	2. Üretim durdurulmuştur, ancak destek süresi devam etmektedir. 3. Destek süresi sona ermiştir. 4. Eski ürünler (makineler) (artık üretilmeyen ve uygun olmayan), eski ürünler için yedek parçalar hariç tutulur. Yedek parçalar: 1. "aynı" = "orijinal": parçalar, CRA'ya uygun olabilmeleri için her ayrıntıda (ör. özellikler, işlevler, bileşenler) aynı olmalıdır. *Örnek: Aynı Parça Numarası – aynı malzeme listesi.* 2. "Aynı özelliklere göre üretilmiş": parça, üçüncü bir tarafça (yasal bir anlaşma kapsamında) veya orijinal üretici tarafından üretilebilir. *Örnek: Üretici, maliyet nedenleriyle bir bileşenin üretimini dış kaynaklara yaptırmaya başlar veya tedarikçiyi değiştirir.* 3. Bir yedek parçanın değiştirilmesi gerekiyorsa (örneğin, bir donanım bileşeninin eskimesi nedeniyle), artık aynı kabul edilemez. Makine üreticisi, değişikliğin önemli bir değişiklik olup olmadığını değerlendirmeli ve CRA teknik belgelerini (örneğin malzeme listesi) buna göre güncellemelidir. Not: Yedek parça üçüncü bir tarafça üretilmiş veya tasarlanmış ve üretilmişse, makinenin uygunluğunu değerlendirmek için (bkz. madde 3) bir değişiklik gerektiğinde (örneğin, bileşenin üretimden kaldırılması nedeniyle) OEM'e bilgi verilmelidir.
Madde 2 (7)	Bu Yönetmelik, münhasıran ulusal güvenlik veya savunma amaçları için geliştirilen veya değiştirilen dijital unsurlar içeren ürünlere veya gizli bilgileri işlemek için özel olarak tasarlanmış ürünlere uygulanmaz.	Ulusal güvenlik / Savunma istisnası.

Madde 2 (8)	Bu Tüzükte belirtilen yükümlülükler, açıklanması üye devletlerin ulusal güvenliği, kamu güvenliği veya savunması ile ilgili temel çıkarlarına aykırı olacak bilgilerin sağlanmasını gerektirmez.	Makine ile ilgili değildir.
Madde 3	**Tanımlar**	
Madde 3. nokta (1)	**"dijital unsurlar içeren ürün"** ayrı olarak piyasaya sürülen yazılım veya donanım bileşenleri dahil olmak üzere, bir yazılım veya donanım ürünü ve bunun uzaktan veri işleme çözümlerini ifade eder;	1. Uzaktan veri işlemenin varlığı, bir yazılım veya donanım ürününün dijital unsurlar içeren ürün olarak kabul edilmesi için ön koşul değildir. 2. Uzaktan veri işleme mevcutsa, risk değerlendirmesinin kapsamına girer. 3. Aşağıdaki tanıma göre yedek parça olarak sınıflandırılmayan yazılım veya donanım bileşenleri, ayrı olarak piyasaya sürüldüklerinde dijital unsurlar içeren ürünler olarak kabul edilir.
Madde 3. madde (2)	"**uzaktan veri işleme"** yazılımın üretici tarafından veya üreticinin sorumluluğu altında tasarlanıp geliştirildiği ve bu özelliğin bulunmaması durumunda dijital unsurlar içeren ürünün işlevlerinden birini yerine getiremeyeceği uzaktan veri işlemeyi ifade eder.	Varsayım: Makine bağlamında, tanımdaki "dijital unsurlar içeren ürün" tüm makineyi ifade eder. Uzaktan veri işleme: 1. Makineye harici (makineye monte edilmemiş) bir donanımda çalışan, yani makineden fiziksel olarak uzakta, uzaktan çalışan bir yazılım. 2. Makineye veri alabilen ve/veya makineye veri gönderebilen bir yazılım. 3. 2. maddede belirtilen yeteneklerin bulunmaması, makinenin amaçlanan işlevlerinden birini (yani, üretici tarafından tanımlanan ve/veya kullanım kılavuzunda ve/veya servis kılavuzunda yer alan amaçlanan işlev) yerine getirmesini engeller. 4. 2. maddede belirtilen yazılım, üretici tarafından veya üreticinin sorumluluğu altında veya üretici adına geliştirilmiştir (makinenin CE işareti, uzaktan veri işlemenin uygunluğunu da kapsar).
Madde 3. madde (4)	**"Yazılım",** bilgisayar kodundan oluşan bilgisayar kodundan oluşan elektronik bilgi sisteminin bir parçasını ifade eder;	Varsayım: Makine bağlamında, yazılım, makinenin donanımı üzerinde çalışabilen bilgisayar kodu bileşenlerini ifade eder (Madde 3. madde (5) uyarınca). Bu Donanım,

		AB pazarına sunulduğu anda makineye fiziksel olarak monte edilen bileşenlerden oluşur.
Madde 3. madde (5)	**"donanım"** , , fiziksel elektronik bilgi sistemi veya dijital verileri işleyebilen, depolayabilen veya iletebilen parçaları;	Varsayım: Makine bağlamında, donanım, makinenin elektronik bilgi sisteminin fiziksel kısmıdır ve makine AB pazarına sunulduğunda fiziksel olarak makineye monte edilen bileşenlerden oluşur.
Madde 3. madde (6)	**"**bile**şen",** yazılım veya elektronik bilgi sistemine entegre edilmesi amaçlanan donanımdır;	1. Bitmiş üründen ayrı olarak piyasaya sürülen bir bileşen, dijital unsurlar içeren bir ürün olarak kabul edilir ve CE işareti gerektirir (bkz. Madde 3.madde (1) bendi). 2. AB pazarına ayrı olarak sunulmayan, bir makineye entegre edilmiş (makinenin elektronik bilgi sistemine entegre edilmiş) bir bileşen, dijital unsurlar içeren bağımsız bir ürün olarak kabul edilmez ve CE işareti gerektirmez.
Madde 3. madde (7)	**"elektronik bilgi sistemi"** dijital verileri işleyebilen, depolayabilen veya iletebilen elektrikli veya elektronik ekipmanları içeren bir sistem anlamına gelir;	Elektronik bilgi sistemi, ilgili bölümlerde tanımlanan donanım ve yazılım bileşenlerinden oluşan bir sistemdir (yazılım, donanım ve bileşen tanımlarına bakınız).
Madde 3. madde (8)	**"mantıksal bağlantı" yazılım arayüzü aracılığıyla** gerçekleştirilen bir veri bağlantısının sanal bir yazılım arayüzü aracılığıyla gerçekleştirilen veri bağlantısının temsilidir;	Mantıksal bağlantı, yazılım bileşenleri arasında dijital veri iletişimini sağlayan bir yazılımdır. Örnek: - bir yazılım protokolü (ör. VPN, IP).
Madde 3. madde (9)	**"fiziksel** bağlantı**"**, fiziksel araçlar kullanılarak, elektriksel, optik veya mekanik arayüzler, kablolar veya radyo dalgaları dahil olmak üzere, elektronik bilgi sistemleri elektriksel, optik veya mekanik arayüzler, kablolar veya radyo dalgaları dahil olmak üzere fiziksel araçlar kullanılarak uygulanan elektronik bilgi sistemleri veya bileşenleri arasındaki bağlantı anlamına gelir;	Tanım kendinden anlaşılırdır. Not: Tanım, fiziksel bileşenler arasındaki bağlantılarla sınırlı değildir.
Makale 3. madde (10)	**"dolaylı bağlantı"** , bir bir cihaza veya ağa doğrudan değil, bu cihaza veya ağa doğrudan bağlanabilen daha büyük bir sistemin parçası olarak yapılan bağlantı;	Tanım kendinden anlaşılırdır.
Madde 3. madde (23)	**"amaçlanan** kullanım**"**, dijital	Kullanım amacı, bir ürünün genel ve üst düzey bir description of a product's function,

	ürünün kullanım kılavuzunda, tanıtım veya satış materyallerinde ve beyanlarında ve teknik belgelerde üretici tarafından sağlanan bilgilerde belirtilen belirli bağlam ve kullanım koşulları dahil olmak üzere, üretici tarafından amaçlanan kullanımdır.	makul olarak öngörülebilen koşullar da dahil olmak üzere. Bu, ürünün son kullanımıdır. Örnek: Bir tarım biçerdöverinin kullanım amacı, çalışma fonksiyonları etkinleştirilmiş halde tarlada mısır hasadı yapmak veya çalışma fonksiyonları devre dışı bırakılmış halde yollarda sürüş yapmaktır.
Madde 3. madde (24)	**"makul öngörülebilir kullanım'** üretici tarafından sağlanan amaçlanan kullanım üretici tarafından sağlanan kullanım, tanıtım veya satış materyallerinde ve ifadelerin yanı sıra teknik dokümantasyon, ancak olasılıkla makul öngörülebilir insan davranışları veya teknik işlemler veya etkileşimler;	Bu, [kullanıcılara yönelik talimatların] bir parçası olabilir. (Ek II) kullanım anlamına gelir. teknik belgelerde bulunabilir (Ek VII). Hazır bulunan özellikler, örneğin mevcut fiziksel bağlantı noktası kullanımının iletişim yeteneği olup olmayan üretici tarafından öngörülen (örneğin, ECU JTAG/Hata Ayıklama portu aracılığıyla donanım yazılımı).

"Makul olarak öngörülebilir kullanım" ile "makul olarak öngörülebilir kötüye kullanım" arasındaki farkı daha iyi anlamak için, "makul olarak öngörülebilir kötüye kullanım"ın tanımı şöyledir:

Madde 3. madde (25)	**"makul olarak öngörülebilir kötüye** kullanım" , dijital unsurlar içeren bir ürünün, amaçlanan kullanım amacına uygun olmayan, ancak makul olarak öngörülebilir insan davranışından veya diğer sistemlerle etkileşimden kaynaklanabilecek şekilde kullanılması anlamına gelir;	"Makul olarak öngörülebilir kötüye kullanım", kullanıcı talimatlarında veya üretici tarafından hazırlanan teknik belgelerde belirtilmemiştir. Yalnızca kullanım amacı ve ortamının dışında meydana gelen ve kullanıcı davranışına veya ürün özelliklerine dayalı olarak öngörülemeyen davranışları ifade eder. Kötüye kullanım, üretici tarafından sağlanan talimatlara uyulduğunda kullanıcı açısından olası veya makul olmayan bir durumdur. Örneğin, bir saldırı için tipik bir kullanıcının sahip olduğu bilginin ötesinde, son derece gelişmiş ve özel bilgi gerekiyorsa, bu durum kötüye kullanım olarak kabul edilir.

Konu: Önemli değişiklik

Madde 3, madde 30	"**Ö**nem**li** değişiklik", dijital ürünlerde yapılan değişiklik yerleştirilmesinden sonra gelen unsurlar	Önemli bir değişiklik, aşağıdaki özelliklere sahip bir değişikliktir: - -

	pazarın temel siber güvenlik gerekliliklerine uygunluğunu etkileyen veya dijital unsurlar içeren ürünün değerlendirildiği amaçta değişikliklere yol açan bir değişikliktir;	siber güvenlik gerekliliklerine uyumu etkileyen (yani yeni bir risk getiren) değişiklik. – nihai ürünün amaçlanan amacını değiştirir (Amaçlanan Amaç tanımına göre). Ayrıca: – Herhangi bir değişiklik için, değişikliğin CRA'nın temel gerekliliklerine uygunluğu tehlikeye atıp atmadığını değerlendiren bir etki analizi yapmak değiştiren kişinin sorumluluğundadır. – Etki analizinin sonuçları, değişiklik önemli bir değişiklik olmasa bile (örneğin, SBOM veya Risk değerlendirmesinin güncellenmesi) belgelendirilmelidir. – Amaçlanan amaç değiştirilirse (Amaçlanan Amaç tanımına göre), mevcut uygunluk artık geçerli değildir. – Değişiklik önemli bir değişiklik ise, her zaman yeni bir uygunluk değerlendirmesi gerekir. Önemli bir değişikliğin ürün uygunluğuna etkisi hakkında daha fazla bilgi için, Mavi Kılavuz'un 2.1 bölümündeki "*Ürünlerin onarımı ve değiştirilmesi*" başlığına bakınız.

Konu: Önemli ve Kritik Ürünler

Referans CRA	**CRA 2024/2847 metni**	**CEMA yorumu**
Madde 7 ve ilgili ekler	**Dijital unsurları içeren önemli ürünler**	
Madde 7 (1)	1. Dijital unsurlar içeren ve Ek III, dijital unsurlar içeren önemli ürünler olarak kabul edilecek ve 32. maddenin 2. ve 3. fıkralarında belirtilen uygunluk değerlendirme prosedürlerine tabi tutulacaktır. Ek III'te belirtilen bir ürün kategorisinin temel işlevselliğine sahip dijital unsurlar içeren bir ürünün entegrasyonu **kend**isi **entegre edildiği ürünün**	Ek III'te listelenen önemli bir ürün olarak nitelendirilen bir bileşen, kendi başına önemli bir ürün olmayan (Ek III'te açıklanan temel işlevselliğe sahip olmadığı için) bir bitmiş ürüne entegre edildiğinde, bitmiş ürün entegrasyon için üretilen bileşenin uygunluk değerlendirme prosedürünü benimsemez/devralmaz. Ek III Sınıf I veya Sınıf II bileşeni içeren bir bitmiş ürün AB'ye ithal edildiğinde ve bileşen ayrı olarak değil,

	uygunluk değerlendirme prosedürleri uygulanır.	ürünle birlikte sunulursa, bitmiş ürünün uygunluk değerlendirme prosedürü bileşeni de kapsar. Böyle bir durumda, bileşenin ayrı olarak sertifikalandırılması gerekmez (CE işareti). Bitmiş ürünün üreticisi, o bileşen için Ek III Sınıf I veya Sınıf II ürünlere (veya ilgili dikey uyumlaştırılmış standarda) uygulanabilir teknik şartnamelere uymak zorundadır. "Temel işlevsellik", üretici tarafından tanımlanır ve ürünün temel, en temel amacını, müşterinin ürünü satın alma nedenini ifade eder. Temel işlevselliği anlamak, pazarlamacıların ürünün değer önerisini etkili bir şekilde iletmelerine ve bunu müşteri beklentileriyle uyumlu hale getirmelerine yardımcı olur. Bazı bileşenler ise özellikler olarak değerlendirilmelidir: bunlar, ürünün kullanılabilirliğini veya değerini artıran belirli işlevler veya özelliklerdir. Temel işlevsellik, bu özelliklerin var olmasının temel nedenini temsil eder. Bu özellikler, temel işlevselliğin kendisi için gerekli değildir.
Ek III		Ek III'teki önemli ürünler listesi kapsamlıdır ve yalnızca delege edilmiş bir kanunla genişletilebilir.
Ek III Sınıf I	14. Güvenlikle ilgili işlevlere sahip mikrodenetleyiciler	Bu, mantıksal saldırılara karşı koruma sağlamak için yerleşik HSM içeren bir mikrodenetleyicidir.
Ek III Sınıf II	4. Kurcalamaya dayanıklı mikrodenetleyiciler	Bu, (mantıksal ve) fiziksel saldırılara karşı koruma sağlamak için yerleşik HSM içeren bir mikrodenetleyicidir.
Madde 8 ve ilgili ekler	**Kritik ürünler ile dijital elemanları**	
Madde 8 (1)	... Bu fıkranın birinci paragrafında atıfta bulunulan delege edilmiş kanunlar kabul edilmemişse, Ek IV'te belirtilen bir ürün kategorisinin temel işlevselliğine sahip dijital unsurlar içeren ürünler, bu paragrafın birinci fıkrasında belirtilen delege edilmiş işlemler kabul edilmemişse, Ek IV'te belirtilen bir ürün kategorisinin temel işlevine sahip dijital unsurlar içeren ürünler	Bu paragraf, CSA 2019/881 kapsamındaki bir siber güvenlik planının kapsamına giren ürünleri de hedeflemektedir. Bu, son derece kritik bir sektörün (NIS2 2022/2555'te tanımlandığı şekliyle) temel bir kuruluşunda kullanılan ürünlerle ilgilidir. NIS2, ürünlere değil **kuruluşlara** uygulanır. Ek IV'te listelenen kritik ürün olarak nitelendirilen bir bileşen,

		(Ek IV'te açıklanan temel işlevselliğe sahip olmadığı için) kritik bir ürün olmayan bir bitmiş ürüne entegre edildiğinde, bitmiş ürün entegrasyon için üretilen bileşenin uygunluk değerlendirme prosedürünü benimsemez/devralmaz.
Ek IV	1. Güvenlik Özellikli Donanım Cihazları Kutular	Bunun kapsam dahilinde olmadığını anlıyoruz kapsamına girmediğini anlıyoruz. "Güvenlik Kutuları ile Donanım Cihazları" , bir bir bir (ICT) (Bilgi ve) ürünleri fiziksel güvenlik önlemleri içerir korumak için tasarlanmış fiziksel güvenlik önlemleri içeren erişime karşı korumak için tasarlanmış fiziksel güvenlik önlemleri içerir. Bu cihazlar genellikle veri güvenliğinin kritik olduğu ortamlarda kullanılır. finansal hizmetler, kamu sektörü ve diğer yüksek güvenlikli sektörler. Bu güvenlik programı EUCC (2019/881 2019/881) "ICT ürünlerini içeren Donanım Cihazları Güvenlik Kutuları"nı kapsar ve bu kutular, kapsamına giren "Güvenlik Kutulu Donanım Cihazları"nı kapsar. Bağlantıya bakınız ENISA – Saldırı Potansiyelinin Uygulanması Potansiyelinin Uygulanması: Güvenlik Kutulu Donanım Cihazları : https://certification.enisa.europa.eu/publications/application-attack-potential-hardware-devices-security-boxes_en

Konu: OEM–Tedarikçi İlişkisi

Madde 13	**Üreticilerin Yükümlülükleri**	
Madde 13 (5)	1. paragrafa uymak amacıyla, üreticiler üçüncü taraflardan temin edilen bileşenleri **entegre ederken**, **bu bileşenlerin** ürünün **siber güvenliğini tehlikeye atmaması** için **gerekli özeni** göstermelidir ticari faaliyet kapsamında piyasaya sunulmamış ücretsiz ve açık kaynaklı yazılım bileşenlerini entegre ederken de dahil olmak üzere, dijital unsurlarla	Bitmiş ürünün üreticisi (OEM), "*kombinasyonu oluşturan uygun ürünleri seçmekten, kombinasyonu ilgili yasaların hükümlerine uygun şekilde bir araya getirmekten ve montajla ilgili mevzuatın tüm gerekliliklerini yerine getirmekten sorumludur*" (bkz. Mavi Kılavuz: 2.1. Ürün kapsamı - Birlik uyumlaştırma mevzuatında ürün kapsamı). *Kombinasyon* terimi, bileşenlerin bitmiş ürüne entegrasyonu olarak yorumlanır. *"Üreticiler, bileşenleri ve parçaları, bitmiş ürünün*

		uygun olacak şekilde seçmelidir." (Bkz. Mavi Kılavuz: 2.1. Ürün kapsamı - Birlik uyum mevzuatında ürün kapsamı). OEM'in risk değerlendirmesi, hangi özelliklerin gerekli olduğunu ve sunulan bileşen özelliklerinin uygunluğa uygun olup olmadığını belirler. Bileşenin tedarikçisi, entegratörün (OEM) gerekli özeni göstermesi için yeterli bilgiyi sağlamalıdır. Bir bileşenin tedarikçisi, sözleşmede belirtildiği şekilde veya bileşen Avrupa pazarına ilk kez sunulduğunda yasal bir yükümlülük olarak, güvenlik açığı yönetimi (bkz. Ek I'in II. Kısmı) dahil olmak üzere sağlanan özelliklerden sorumludur. Bitmiş ürünün üreticisi (OEM), bitmiş ürünün genel uyumluluğundan sorumlu olmaya devam eder. Bu, tedarikçinin talimatlarına göre bitmiş ürünün varsayılan olarak güvenli yapılandırılmasını sağlamak için bileşenin güvenlik özelliklerinin etkinleştirilmesini içerir (Ek II, madde 8 (f)). <u>Bileşenin CRA uyumlu olması gereken durumlar:</u> Durum tespiti (bkz. Gerekçe 34), OEM'in gerekli güvenlik özelliklerine sahip bileşenleri seçmesini ve bileşenin uygunluk beyanının CRA'yı kapsayıp kapsamadığını doğrulamasını gerektirir. OEM, bu bileşeni tedarikçinin talimatlarına uygun olarak bitmiş ürüne entegre etmeli ve yapılandırmalıdır (bkz. Ek II). <u>Bileşenin bir sözleşme kapsamında olması ve CRA ile uyumlu olması gerekmemesi durumu:</u> Bileşen entegrasyon için üretilmişse ve AB pazarında ayrı olarak satılmıyorsa, OEM, bileşen dahil bitmiş ürünün CRA'ya uygun olmasını sağlamalıdır. CE işareti sadece bitmiş ürün düzeyinde geçerlidir, bileşen düzeyinde geçerli değildir. Sorumlulukların paylaşımı bir sözleşmede belirtilebilir.
Madde 13 (6)	Üreticiler, dijital elemanlarla ürüne entegre edilmiş bir bileşende, açık kaynak bileşenler de dahil olmak üzere, bir güvenlik açığı tespit ettiklerinde, bu güvenlik açığını bileşeni üreten veya bakımını yapan kişi veya kuruluşa bildirmelidir. veya bileşeni bakımını yapan kişi veya kuruluşa bildirmelidir.	Bitmiş ürünün üreticisi bir bileşende bir güvenlik açığı tespit ettiğinde, bu durum iletilmeli ve tedarik zincirinden bir tepki almalıdır. Güvenlik açığı daha sonra ele alınmalı ve giderilmelidir.

	Güvenlik açığını, Ek I'in II. Kısmında belirtilen güvenlik açığı ele alma gerekliliklerine İkinci bölümde belirtilen güvenlik açığı ele alma gerekliliklerine **uygun olarak** ele alınmalı ve giderilmelidir. **Üreticiler, söz konusu bileşendeki güvenlik açığını gidermek için bir yazılım veya donanım değişikliği geliştirdiklerinde, ilgili kodu veya belgeleri kişi veya kuruluşla paylaşmalıdır.**	CRA uyumlu bir bileşenin tedarikçisi, tanımlanan destek süresi içinde destek sağlayamaz hale gelirse (örneğin, tedarikçinin faaliyetine son vermesi nedeniyle) ve başka hiçbir tüzel kişilik sorumluluğu üstlenmezse, nihai ürünün üreticisi uygun bir çözüm bulmaktan sorumlu hale gelir. Bu gibi durumlarda, tedarikçinin tüm kaynak kodunu ve gerekli bilgileri nihai ürünün üreticisine sözleşme yoluyla sağlaması ve böylece üreticinin kendi düzeltme işlemlerini gerçekleştirebilmesi tavsiye edilir. Ücretsiz ve açık kaynaklı yazılım bileşenleri veya AB dışından temin edilen bileşenler için, tespit edilen tüm güvenlik açıklarının giderilmesinden her zaman nihai ürünün üreticisi sorumludur.
İlgili gerekçeler		
Gerekçe (34)	**tasarım ve geliştirme aşamasında** dijital unsurlar içeren ürünlere **üçüncü taraflardan temin edilen bileşenlerin entegre edilmesi**, üreticiler, ürünlerin **tasarlanması, geliştirilmesi ve üretilmesini** sağlamak için bu Yönetmelikte belirtilen temel siber güvenlik gerekliliklerine uygun olarak bu bileşenlerle ilgili olarak, **piyasada bulunmayan ücretsiz ve açık kaynaklı yazılım bileşenleri dahil olmak üzere, bu bileşenlere ilişkin gerekli özeni göstermelidir**. **Uygun özen düzeyinin** belirli bir bileşenle ilişkili siber güvenlik riskinin niteliğine ve düzeyine bağlıdır ve bu amaçla uygun olduğu şekilde, **bileşenin üreticisinin bu Yönetmeliğe uygunluğunu kanıtladığını** doğrulamak**, buna bileşenin halihazırda CE işaretini taşıyıp taşımadığını kontrol etmek de dahildir**; **bileşenin düzenli güvenlik güncellemeleri aldığını** doğrulamak**, örneğin güvenlik güncelleme geçmişini kontrol etmek**; **bileşenin** **bileşeninin free from**	Dijital unsurlar içeren bir ürün olan bitmiş ürünün üreticisi, ücretsiz ve açık kaynaklı yazılımlar da dahil olmak üzere, entegre üçüncü taraf bileşenler için temel siber güvenlik gerekliliklerini karşılamak üzere gerekli özeni göstermelidir. Durum tespiti, AB pazarına sunulan dijital unsurlar içeren bileşenler üzerinde bitmiş ürünün üreticisi (OEM) tarafından gerçekleştirilir. Bu bağlayıcı olmayan gerekçe, uyumluluğu sağlamak için aşağıdaki eylemlerden bir veya daha fazlasının dikkate alınmasını önerir: • Uygulanabilir olduğu durumlarda, CE işaretini kontrol ederek bileşenlerin uygunluğunu doğrulamak, • Düzenli güvenlik güncellemeleri yapma kapasitesinin sağlanması, • Halka açık güvenlik açığı veritabanlarında güvenlik açıkları olup olmadığını kontrol etmek, • Ek güvenlik testleri yapmak, • Tedarikçinin talimatlarına göre bitmiş ürünün varsayılan olarak güvenli yapılandırılmasını sağlamak için bileşen güvenlik özelliklerini etkinleştirme. Bitmiş ürünün üreticisi bir güvenlik açığı tespit ederse, bu durum bildirilmeli ve tedarik zincirinden bir tepki alınmalıdır.

	Direktif (AB) 2022/2555'in 12(2) maddesi uyarınca oluşturulan Avrupa güvenlik açığı veritabanında veya diğer kamuya açık güvenlik açığı veritabanlarında kayıtlı güvenlik açıkları; **veya ek güvenlik testleri** yapmak. **Güvenlik açığı ile ilgili yükümlülükler** bu Yönetmelik, üreticilerin dijital unsurlar içeren bir ürünü piyasaya sürerken ve destek süresi boyunca uymak zorunda oldukları **dijital unsurlar içeren ürünlerin tamamına, tüm entegre bileşenler dahil olmak** üzere **uygulanır**. , dijital unsurlar içeren ürünün üreticisi bir bileşende, **ücretsiz ve açık kaynaklı bileşenler dahil olmak üzere**, bir güvenlik açığı tespit ederse, **bileşeni üreten veya bakımını yapan kişi veya kuruluşa bilgi vermeli**, güvenlik açığını gidermeli uygulanabilir durumlarda, ilgili kişi veya kuruluşa kuruluşa uygulanan güvenlik düzeltmesini sağlamalıdır.	Güvenlik açığı giderilmeli ve düzeltilmelidir. CRA uyumlu bir bileşenin tedarikçisi destek süresi içinde artık destek sağlayamıyorsa (örneğin, tedarikçinin iflas etmesi nedeniyle) ve başka hiçbir tüzel kişilik sorumluluğu üstlenmiyorsa, nihai ürünün üreticisi sorumlu hale gelir ve uygun bir çözüm bulmalıdır. Bu gibi durumlarda, tedarikçinin tüm kaynak kodunu ve gerekli bilgileri nihai ürünün üreticisine sözleşme yoluyla sağlaması ve böylece üreticinin kendi düzeltmesini yapabilmesi tavsiye edilir. Ücretsiz ve açık kaynaklı yazılım bileşenleri veya AB dışından temin edilen bileşenler için, nihai ürünün üreticisi her zaman güvenlik açıklarını gidermekten sorumludur.
Gerekçe (64)	... Üreticiler, yalnızca belirli bir amaca uygun olarak özel olarak tasarlanmış ürünlerle ilgili temel siber güvenlik gerekliliklerinden sapma yapabilmelidir. belirli bir ticari kullanıcı ve **hem üretici hem de kullanıcı farklı bir sözleşme şartları setini açıkça kabul etmişse**.	"Özel üretim ürün", bu Yönetmelik kapsamına giren (CRA uyumluluğuna tabi) bir üründür ve bir OEM (ticari kullanıcı olarak) tarafından bitmiş bir ürüne entegre edilmek üzere üretilen ve CRA temel gerekliliklerinden sapmaların sözleşme ile kararlaştırılabileceği bileşenleri içerir. Not: 2 veya daha fazla ekonomik operatör arasında "ortak tasarım" yoluyla geliştirilen ürünler "özel üretim ürünler" olarak kabul edilmez. Entegrasyon için üretilen ve "ortak tasarım" yoluyla geliştirilen bu tür bileşenler, CRA'nın kapsamı dışında tutulur. Piyasaya sürülme ile ilgili Mavi Kılavuz bölüm 2.3'e de bakınız: "*Bazen ürünler sipariş verildikten sonra üretilir. Üretim aşaması tamamlanmadan önce yapılan bir teklif veya anlaşma, piyasaya sürülme olarak kabul edilemez (örneğin, sözleşmenin tarafları tarafından kararlaştırılan belirli şartnamelere göre bir ürünün üretilmesi için yapılan teklif, ürünün ancak daha sonraki bir aşamada üretilip teslim edileceği durumlarda)*."

İlgili Ekler		
Ek I bölüm 1 (2) (b)	Siber güvenlik temelinde risk değerlendirmesi için Madde 13(2)'de belirtilen ve uygun olduğu durumlarda, ürünlerin yapılandırması: ... piyasada ile bir güvenli tarafından varsayılan yapılandırma, aksi üretici ile üretici ile iş kullanıcısı, dijital öğelerle dijital öğeler içeren özel yapım ürünle ilgili ürünü orijinal durumuna sıfırlama olasılığı dahil orijinal durumuna sıfırlama olasılığı dahil;	Nihai ürün için metin açıktır, ancak açıklama açıklamada açıklamada güvenli varsayılan bileşenlerin yapılandırması ile ilgili olarak, Alt konu: **Tedarikçinin sorumlulukları** **Bileşenler**
Ek II	minimum, ürün ile dijital elemanlar şöyle ayr eşlik eden: ... 8. ayrıntılı talimatlar veya internet adresini içermelidir. talimatlar ve bilgiler: ... (f) Dijital dijital unsurlar içeren ürünün diğer dijital unsurlar içeren ürünlere entegre edilmesi amaçlanıyorsa, entegratörün g**erek**li **bilgileri** **uygunluğu gerekli siber güvenlik** **gerek**li**liklerine** uyması için gerekli olan Ek VII'de belirtilen belgeleme gereklilikleri.	Bu, yerleştirilen bileşenlerle ilgilidir AB'de bitmiş üründen ayrı olarak pazar. Entegrasyon için üretilen bu tür bileşenler için, tedarikçi, yeterli talimatlar sağlamalıdır bileşenin entegr a s yonu, aşağıdakilerle ilgili üretici adresinden adresinden adresinden adresinden adresinden adresinden gerekli özeni gösterir (bkz. gerekçe 34).

Konu: Bileşen Tedarikçisinin Sorumlulukları

Siber Dayanıklılık Yasası (CRA) şunları gerektirir:

- Dijital unsurlar içeren ürünleri piyasaya sunarken varsayılan olarak güvenli bir yapılandırma (Ek I, Kısım I, madde (2)(b)).
- Dijital unsurlar içeren ürünlerin tasarımı ve üretimi sırasında risklere dayalı uygun düzeyde siber güvenlik (Ek I, Bölüm I, madde (1)).

CRA'nın "dijital unsurlar içeren ürün" tanımı, bileşenleri de içerir; bu, bileşenlerin CRA'nın kapsamına girdiğini anlamına gelir.

Aşağıdaki kılavuz, entegrasyon için üretilen bileşenlerin üreticilerine (tedarikçilerine) yukarıda belirtilen temel siber güvenlik gereklilikleriyle ilgili **iki önemli soruyu** ele almalarına yardımcı olmak amacıyla hazırlanmıştır:

1. Bir tedarikçi, OEM tarafından nihai ürüne entegrasyonunu kolaylaştırmak için, "varsayılan olarak güvenli yapılandırmaya" sahip olmayan, entegrasyon için üretilmiş bir bileşeni piyasaya sunabilir mi?
2. Bir tedarikçi, farklı güvence seviyelerine sahip (entegrasyon için üretilmiş) hazır bileşenleri piyasaya sunabilir mi?

Bu tartışmalarla ilgili olarak, öncelikle "*entegrasyon için bileşen*" ve "*nihai ürün*" terimlerinin ne anlama geldiği açıklığa kavuşturulmalıdır.

- CRA'ya göre **"bileşen"**, dijital öğelerle (PDE) bir ürüne **entegre edilmesi amaçlanan** ve siber güvenlikle ilgili olan herhangi bir yazılım veya donanım öğesidir. Bu nedenle, **"**entegrasyon **için üretilmiş bileşen"**
  piyasaya tek başına, müşteriye kullanıma hazır bir ürün (nihai ürün) olarak sunulmak üzere değil, diğer ürünlerin üreticileri (iş kullanıcıları) tarafından kullanılan bir yapı taşı olarak sunulmak üzere tasarlanmıştır. Son kullanıcı, bileşeni yalnızca nihai ürüne entegre edilmiş olarak kullanacaktır.
- **Nihai ürün**[2] : bağımsız, müşteriye hazır bir ürün anlamına gelir, bu nedenle
  doğrudan son kullanıcı (örneğin çiftçi) tarafından kullanılmak üzere tasarlanmıştır.

1. Bir tedarikçi, OEM tarafından nihai ürüne entegrasyonunu kolaylaştırmak için, "varsayılan olarak güvenli olmayan bir yapılandırmaya" sahip, entegrasyon için üretilmiş bir bileşeni piyasaya sunabilir mi?

Cevap EVET'tir.

Bunun temel gerekçesi, entegrasyon sırasında zaten güvenli bir şekilde yapılandırılmış bileşenleri entegre etmenin zor olması ve ek adımlar gerektirmesidir. Bu, bileşenlerin entegrasyonunu gereksiz yere karmaşık hale getirir ve entegrasyon sırasında ekstra saldırı yüzeyi ortaya çıkarabilir. Bileşen tek başına kullanıldığında risk oluşturmadığından, entegrasyondan önce güvenlik yapılandırması gerekmez.
Bileşenleri güvenli bir yapılandırma olmadan piyasaya sunmak, aşağıdaki örneklerde gösterildiği gibi bu karmaşıklığı önemli ölçüde azaltır:

- Kripto modülü içeren bir ECU, gizli anahtarlar olmadan ve ayrıcalıklı işlevler devre dışı bırakılmış olarak gönderilir. OEM, entegrasyon sırasında anahtarları sağlayabilir ve güvenlik özelliklerini etkinleştirebilir (kimlik doğrulama gerekmez).
- Güvenli Önyükleme özelliğini içeren ve uygulama olmadan (yalnızca minimal önyükleyici ile) teslim edilen bir ECU. OEM, güvenliği devre dışı bırakmadan veya güven kökünü değiştirmeden uygulamayı flashlayabilir ve güven kökünü sağlayarak güvenli önyüklemeyi etkinleştirebilir.

Madde 13 ve Ek II, madde 8(f) ile ilgili olarak ana koşul, tedarikçinin "*entegratörün temel siber güvenlik gerekliliklerine uyması için gerekli bilgileri*" sağlamasıdır.
Entegrasyon için üretilen bir bileşen, yapılandırılmadan piyasaya sunulursa, tedarikçi, güvenlik özelliklerinin düzgün bir şekilde etkinleştirilmesi için OEM'e (bileşeni entegre eden aracın üreticisi) güvenli bir şekilde nasıl yapılandırılacağını bildirmelidir. Tüm güvenlik özellikleri,

---

[2] Mavi kılavuzda bir bileşen, kılavuzda yalnızca iki koşuldan bahsedildiği için bitmiş bir ürün olarak görülebilir:

- Tamamen üretilmiş ve dağıtım için hazır.
- Tedarik zincirine girmiş (yani başka bir tarafa aktarılmış), AB pazarına resmi girişini işaret eden. Bu nedenle, bitmiş ürün yerine nihai ürün terimi kullanılmaktadır.

Tedarikçi tarafından yapılan risk değerlendirmesine göre gerekli olan, bileşenin piyasaya sunulduğu anda mevcut olmalıdır.
Bu kılavuzlar, nihai ürünü müşteriye varsayılan olarak güvenli bir yapılandırma ile teslim etmek için temel gerekliliklerin amacına uygundur.

2. Bir tedarikçi, farklı güvence seviyelerine sahip hazır bileşenleri (entegrasyon için üretilmiş) piyasaya sürebilir mi?

Cevap evettir.

Entegrasyon için üretilen bileşenler, nihai ürünün bir parçası olmak üzere tasarlanmıştır. Entegrasyon için üretilen bileşen ve nihai ürün CRA'nın kapsamına girdiğinden, güvenlik önlemleri bu nihai ürünün mimarisinin farklı düzeylerinde (örneğin, bileşen düzeyinde veya nihai üründe daha üst düzeyde) uygulanabilir.

Örneğin, güvenlikle ilgili verileri işleyen bir bileşen, bir ağ geçidi tarafından korunan özel bir ağda izole edilebilir. Bu durumda ağ geçidi güvenliği üstlenir. Bu nedenle, OEM, farklı güvenlik düzeyleri veya farklı güvence düzeyleri uygulayan bileşenleri piyasada bulabilmelidir.

Her bileşenin, içine yerleştirildiği nihai ürünlerin çalışma ortamı ve güvenlik mimarisinden bağımsız olarak uyumluluk yükümlülüğü, bileşenin aşırı mühendislikle tasarlanmasına neden olabilir.

Yorumumuza göre, CRA, entegrasyon için üretilen bileşenlerin farklı güvence seviyeleriyle piyasaya sürülmesine izin vermektedir. Bu, en uç durumda, risk değerlendirmesinin olası bir sonucu olarak, bileşenin herhangi bir siber güvenlik özelliğine ihtiyaç duymayabileceği anlamına gelebilir.
sonuç olarak bileşenin herhangi bir siber güvenlik özelliğine ihtiyaç duymayabileceği anlamına gelebilir.

Hazır bileşen tedarikçileri, bileşenlerin hangi nihai ürünlere entegre edileceğini her zaman bilmezler. Bu nedenle, tedarikçi, bileşenin kullanılabileceği nihai ürünlerin farklı çalışma ortamlarını kapsayacak şekilde, bileşen düzeyinde aşağıdakileri iyi bir şekilde belgelemelidir:

- Hazır bileşenlerin nihai uygulaması, nihai ürünün çalışma ortamı da dahil olmak üzere bilinmediğinden, tedarikçi yalnızca bileşen sınırları içindeki çalışma ortamı hakkında varsayımlarda bulunabilir

  işletim ortamı hakkında varsayımlarda bulunabilir (CRA Madde 13.3).
- Tedarikçi, **korunacak varlıkları** belirlemek için amaçlanan kullanım ve makul olarak öngörülebilir kullanım[3] (CRA Madde 13.3) temelinde bir risk değerlendirmesi yapmalıdır. Tedarikçi, korumayı sağlamak için uygun risk azaltma önlemleri uygulayabilir **VEYA** entegratörün korumayı sağlayabilmesi için

  entegratörün korumayı sağlamasına olanak tanıyan kalıntı riskler hakkında bilgi sağlamalıdır.
- Ürün entegrasyon için üretilmiş bir bileşen değilse, CRA üreticiden "siber güvenliği sağlamasını" ve güvenlik seviyesini uygun şekilde yükseltmesini ister.
- **Tedarikçi,** kullanıcıya "amaçlanan kullanım", "
  güvenlik ortamı", "temel işlevler ve güvenlik özellikleri hakkında bilgiler" (Ek II 4.), "ürünün amaçlanan kullanımına uygun olarak veya makul olarak öngörülebilir kötüye kullanım koşulları altında dijital unsurlarla birlikte kullanılmasıyla ilgili, önemli siber güvenlik risklerine yol açabilecek bilinen veya öngörülebilir her türlü durum" (Ek II 5.)
- Entegrasyon için üretilen bileşenleri seçerken, nihai ürünün **üreticisi,** tedarikçi tarafından sağlanan **belgeleri dikkatlice inceleyerek** aşağıdakileri sağlamalıdır

[3] Tek bir işlevi olan bileşenler için bu kavramlar birbiriyle örtüşmektedir.

nihai ürününe veya alt sistemine entegre edilecek uygun güvenlik seviyesine sahip **doğru bileşeni seçtiğinden emin olmalıdır.**

- Bileşen seçildikten sonra, üretici bileşenin **doğru yapılandırılması/entegrasyonu için sağlanan bilgileri takip** etmeli ve bileşenin **başarılı bir şekilde entegre edildiğini doğrulamalıdır** (**özen yükümlülüğü**).

Konu: Destek süresi dahil olmak üzere güvenlik açığı işleme süreci

Madde 3	**Tanımlar**	
Madde 3(41)	"ist**ismar edilebilir güvenlik** açığı**",** pratik operasyonel koşullar altında bir düşman tarafından etkili bir şekilde kullanılma potansiyeline sahip güvenlik açığı anlamına gelir;	"Kullanılabilir güvenlik açığı", • bir saldırı yolu vardır ve • saldırı yolu makul bir süre içinde ○ makul bir süre içinde ○ ürünün makul olarak öngörülebilir kullanımı dikkate alındığında (örneğin, ürün sökülmemiştir) ve bunu kullanmak için gerekli bilgi/araçlar ne olursa olsun. Not: güvenlik açıkları veritabanına bağlantılıdır (aktif olarak istismar edildiği bildirilen güvenlik açıkları).
Madde 13-14	**Güvenlik açığı yönetimi/bildirimi** **destek süresi boyunca**	
Madde 14 (1)	Üret**ici**, **aktif olarak istismar edilen güvenlik açığını** üründe bulunan ve dijital unsurlar içeren güvenlik açığını, bu Maddenin 7. paragrafı uyarınca koordinatör olarak atanan CSIRT'ye ve ENISA'ya eşzamanlı olarak bildirmelidir. Üretici, aktif olarak istismar edilen güvenlik açığını, 16. Madde uyarınca oluşturulan tek raporlama platformu aracılığıyla bildirmelidir.	Şu anda, üreticilerin aktif olarak istismar edilen güvenlik açıklarını proaktif olarak izlemeleri için açık bir gereklilik bulunmamakta ve bu tür güvenlik açıklarından nasıl haberdar olmaları gerektiği de açıkça tanımlanmamıştır. Ancak, 11 Aralık 2027 tarihinden itibaren, güvenlik açığı yönetimi gerekliliklerinin uygulanmasıyla gerekliliklerinin uygulanmasıyla birlikte, üreticilerin yeni tespit edilen güvenlik açıklarının ürünleriyle ilgili olup olmadığını değerlendirebilmeleri beklenmektedir. İlgili güvenlik açıkları tespit edildiğinde, üreticiler kullanıcıları bilgilendirmek, güvenlik güncellemeleri yayınlamak veya diğer gerekli önlemleri almak gibi uygun tedbirleri almalıdır. Üretici, aktif olarak istismar edilen bir güvenlik açığının farkına varırsa, ENISA tarafından oluşturulan tek raporlama platformu aracılığıyla bir bildirimde bulunmalıdır. Üretici, güvenlik açığını bildirmek için tek bir irtibat noktası sağlamakla yükümlüdür. (Bu araç, AB Güvenlik Açığı Veritabanından farklıdır ve şu anda bilinmemektedir).

Madde 13 (8)	Üreticiler, dijital unsurlar içeren bir ürünü piyasaya sürerken ve **destek süresi** boyunca, ürünün güvenlik açıklarının etkili bir şekilde ve Ek I'in II. Kısmında belirtilen temel siber güvenlik gerekliliklerine uygun olarak ele alınmasını sağlamalıdır. Üreticiler, özellikle makul kullanıcı beklentilerini, ürünün kullanım amacını da içeren niteliğini ve dijital unsurlar içeren ürünlerin ömrünü belirleyen ilgili Birlik hukukunu dikkate alarak, ürünün kullanım ömrünü yansıtacak şekilde destek süresini belirlemelidir. Destek süresini belirlerken, üreticiler diğer üreticiler tarafından piyasaya sürülen benzer işlevsellik sunan dijital unsurlar içeren ürünlerin destek sürelerini, işletim ortamının kullanılabilirliğini, temel işlevleri sağlayan ve üçüncü taraflardan temin edilen entegre bileşenlerin destek sürelerini ve 52(15) maddesi uyarınca oluşturulan özel idari işbirliği grubu (ADCO) ve Komisyon tarafından sağlanan ilgili kılavuzlar da dikkate alınabilir. Destek süresinin belirlenmesi için dikkate alınacak hususlar, orantılılığı sağlayacak şekilde değerlendirilir. İkinci paragrafa halel getirmeksizin, destek süresi en az beş yıl olmalıdır. Dijital unsurlar içeren ürünün beş yıldan az bir süre kullanılması bekleniyorsa, destek süresi beklenen kullanım süresine karşılık gelmelidir. zaman.	Sektörümüz için **destek süresi**: Aşağıdaki iki koşulun her ikisinin de yerine getirilmesi durumunda en az 10 yıllık destek süresi (OEM kararı): • Temel işlevleri sağlayan entegre bileşenlerin üreticileri bu süre boyunca bilgi sağlamaya devam ederler. VE • uyumluluğu etkileyen dış faktörler güncellemeleri imkansız hale getirmezse (ör. araç zincirinin eskimesi, uzmanlık). Üretici, destek süresine karar verirken, ürünün kullanım ömrü boyunca çalışma ortamında meydana gelebilecek olası değişiklikleri de dikkate alabilir. Ayrıca, güncelleme saklama süresi 10 yıldır ve bu süre boyunca güncellemeler yayınlandıktan sonra indirilip yüklenebilir. Gerekçe: • Birçok tarım traktörünün ömrü daha uzundur; ancak genellikle sadece ilk yıllarda (8 yıla kadar) çiftçiler için ana araç olarak tam kapasiteyle kullanılırlar. Daha sonra genellikle yardımcı araç olarak kullanılırlar. Traktörler, türlerine göre en yüksek sayıda üretilen araçlardır ve bu nedenle olası siber saldırıların birincil hedefi olmaları beklenir. • Bağlantılı tarım makineleri veya traktörlerin sayısı nispeten azdır. Akıllı telefonlar genellikle %100 kablosuz (OTA) güncelleme alırken, tüm portföydeki tarım makineleri ve traktörler için gerçek rakam %20 civarında OTA'dır ve güncellemelerin yaklaşık %80'i bayiler tarafından sağlanmaktadır. Çiftlikler, NIS2 kapsamında önemli veya temel varlıklar olarak kabul edilmez.

CEMA HAKKINDA

CEMA aisbl (www.cema-agri.org), Avrupa tarım makineleri endüstrisini temsil eden bir dernektir. 11 ulusal üye dernekten oluşan CEMA ağı, hem büyük çokuluslu şirketleri hem de
bu sektörde faaliyet gösteren çok sayıda Avrupa KOBİ'sini temsil etmektedir.

CEMA, yaklaşık 450 farklı makine türü üreten, yıllık cirosu yaklaşık 40 milyar avro olan ve 150.000 doğrudan çalışanı bulunan yaklaşık 1.300 üreticiyi temsil etmektedir. CEMA şirketleri, tohumlamadan hasada kadar tarladaki her türlü faaliyeti kapsayan geniş bir makine yelpazesinin yanı sıra hayvancılık yönetimi için ekipmanlar da üretmektedir.

Daha fazla bilgi için lütfen iletişime geçiniz:

CEMA aisbl

Avrupa Tarım Makinaları Endüstrisi Birliği

Avenue de Tervueren 168 1150 Brüksel

Tel. +32 2 706 81 73

secretariat@cema-agri.org