Amtsblatt
der Europäischen Union

DE
Reihe L

2025/2392

1.12.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/2392 DER KOMMISSION

vom 28. November 2025

über die technische Beschreibung der Kategorien von wichtigen und kritischen Produkten mit digitalen Elementen gemäß der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) ([1]), insbesondere auf Artikel 7 Absatz 4,

in Erwägung nachstehender Gründe:

(1) Die Verordnung (EU) 2024/2847 enthält Vorschriften für die Cybersicherheit von Produkten mit digitalen Elementen. Insbesondere enthält Anhang III der genannten Verordnung Kategorien von wichtigen Produkten mit digitalen Elementen, die beim Inverkehrbringen strengeren Konformitätsbewertungsverfahren unterliegen als andere Produkte mit digitalen Elementen. Anhang IV der Verordnung (EU) 2024/2847 enthält die Kategorien von kritischen Produkten mit digitalen Elementen, für die von den Herstellern verlangt werden könnte, im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([2]) ein europäisches Cybersicherheitszertifikat einzuholen oder die beim Inverkehrbringen einer obligatorischen Konformitätsbewertung durch Dritte unterliegen würden.

(2) Nach Artikel 7 Absatz 1 und Artikel 8 Absatz 1 der Verordnung (EU) 2024/2847 bestimmt die Kernfunktion eines Produkts mit digitalen Elementen, ob das Produkt mit digitalen Elementen der technischen Beschreibung einer Kategorie von wichtigen oder kritischen Produkten mit digitalen Elementen entspricht und folglich welchem Konformitätsbewertungsverfahren es unterliegt.

(3) Im Zuge der Entwicklung von Produkten mit digitalen Elementen und um die gewünschten Funktionen zu erzielen, integrieren die Hersteller in ihre eigenen Produkte mit digitalen Elementen üblicherweise andere Komponenten, bei denen es sich ebenfalls um Produkte mit digitalen Elementen handelt und die der technischen Beschreibung einer Kategorie von wichtigen oder kritischen Produkten entsprechen können. Gemäß der Verordnung (EU) 2024/2847 unterliegt ein Produkt mit digitalen Elementen den Konformitätsbewertungsverfahren, die für wichtige oder kritische Produkte mit digitalen Elementen gelten, wenn es sich bei diesem Produkt insgesamt um ein wichtiges oder kritisches Produkt gemäß den Anhängen III und IV der genannten Verordnung handelt. So führt beispielsweise die Integration eines eingebetteten Browsers als Komponente einer Nachrichten-App zur Verwendung mit Smartphones für sich genommen nicht dazu, dass die Nachrichten-App dem Konformitätsbewertungsverfahren unterliegt, das für Produkte mit digitalen Elementen gilt, die die Kernfunktion von „eigenständigen und eingebetteten Browsern“ aufweisen. Dennoch muss der Hersteller gemäß der Verordnung (EU) 2024/2847 sicherstellen, dass das Produkt mit digitalen Elementen insgesamt die grundlegenden Cybersicherheitsanforderungen erfüllt. Daher muss der Hersteller die Sicherheit des gesamten Produkts bewerten und dabei gegebenenfalls die Sicherheit der in das Produkt integrierten Komponenten oder Funktionen berücksichtigen. Damit der Hersteller einer Nachrichten-App beispielsweise die Konformität seines Produkts mit digitalen Elementen mit der Verordnung (EU) 2024/2847 nachweisen kann, muss er nachweisen, dass die Nachrichten-App insgesamt die geltenden Anforderungen erfüllt, wobei gegebenenfalls die Sicherheit des in die App integrierten eingebetteten Browsers zu berücksichtigen ist.

([1]) ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Die Tatsache, dass ein Produkt mit digitalen Elementen im Vergleich zu den technischen Beschreibungen jener Verordnung andere oder zusätzliche Funktionen erfüllt, bedeutet für sich genommen nicht, dass das Produkt mit digitalen Elementen nicht die Kernfunktionen einer in den Anhängen III und IV der Verordnung (EU) 2024/2847 aufgeführten Produktkategorie aufweist. Beispielsweise umfassen Produkte mit digitalen Elementen, die die Kernfunktion von „Betriebssystemen“ aufweisen, häufig Software für Nebenfunktionen, die nicht in der technischen Beschreibung dieser Produktkategorie enthalten sind, wie z. B. Rechner oder einfache Grafikprogramme. Produkte mit digitalen Elementen enthalten häufig auch Komponenten, die die Funktion eines anderen wichtigen oder kritischen Produkts mit digitalen Elementen aufweisen, wie z. B. ein Betriebssystem mit integrierter Browserfunktion oder einen Router mit integrierter Firewall-Funktion. Dies bedeutet jedoch für sich genommen nicht, dass solche Produkte mit digitalen Elementen nicht die Kernfunktion von „Betriebssystemen“ bzw. „Routern, Modems für die Internetanbindung und Switches“ aufweisen.

(5) Ein Produkt mit digitalen Elementen, das die Funktionen einer in den Anhängen III und IV der Verordnung (EU) 2024/2847 aufgeführten Produktkategorie ausüben kann, dessen Kernfunktionen sich jedoch von der einer solchen Produktkategorie unterscheiden, gilt hingegen nicht als ein Produkt, das der technischen Beschreibung dieser Produktkategorie entspricht. So kann beispielsweise eine SOAR-Software (Security Orchestration, Automation and Response) häufig die Funktionen von Produkten mit digitalen Elementen in der Kategorie „Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)“ erfüllen, d. h. Daten sammeln, analysieren und als umsetzbare Informationen für Sicherheitszwecke darstellen. Da ihre Kernfunktion jedoch eine andere als die eines SIEM ist, entspricht SOAR-Software in der Regel nicht der technischen Beschreibung von „Systemen für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)“. Ein ähnliches Beispiel sind Smartphones, da diese üblicherweise Komponenten enthalten, die die Funktionen mehrerer in den Anhängen III und IV der Verordnung (EU) 2024/2847 aufgeführter Produktkategorien ausüben, wie z. B. ein Betriebssystem oder einen integrierten Passwort-Manager. Da die Kernfunktion eines Smartphones jedoch eine andere als die eines Betriebssystems oder eines Passwort-Managers ist, entspricht es in der Regel nicht der technischen Beschreibung dieser Produktkategorien.

(6) Gemäß Artikel 13 Absätze 2 und 3 der Verordnung (EU) 2024/2847 müssen die Hersteller von Produkten mit digitalen Elementen die grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I der Verordnung (EU) 2024/2847 in einer Weise umsetzen, die den Risiken des Produkts mit digitalen Elementen auf der Grundlage der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung sowie der Nutzungsbedingungen des Produkts mit digitalen Elementen unter Berücksichtigung der voraussichtlichen Nutzungsdauer des Produkts angemessen ist. Gemäß Artikel 13 Absätze 2 und 3 der genannten Verordnung und unabhängig davon, ob das Produkt mit digitalen Elementen als wichtiges oder kritisches Produkt mit digitalen Elementen angesehen wird, müssen die Hersteller eine umfassende Bewertung des Cybersicherheitsrisikos durchführen und Angaben dazu machen, wie die grundlegenden Cybersicherheitsanforderungen auf der Grundlage der Risikobewertung umgesetzt werden, sowie zur Erprobung und Vertrauenswürdigkeit. Entspricht die Kernfunktion des Produkts mit digitalen Elementen der technischen Beschreibung eines wichtigen oder kritischen Produkts mit digitalen Elementen, so müssen die Hersteller die Konformität im Rahmen der spezifischen Konformitätsbewertungsverfahren gemäß Artikel 32 Absätze 2, 3, 4 und 5 der Verordnung (EU) 2024/2847 nachweisen.

(7) Jene Verordnung enthält Beispiele für Produkte mit digitalen Elementen, deren Kernfunktion der technischen Beschreibung bestimmter wichtiger oder kritischer Produkte mit digitalen Elementen entspricht. Diese Beispiele dienen lediglich der Veranschaulichung und erheben keinen Anspruch auf Vollständigkeit.

(8) Um den Herstellern Rechtssicherheit zu bieten, sollten die Kategorien von Produkten mit digitalen Elementen, bei denen es sich um manipulationssichere Mikroprozessoren, manipulationssichere Mikrocontroller sowie Chipkarten und ähnliche Geräte, einschließlich Sicherheitselemente, handelt, nach dem Grad der Widerstandsfähigkeit gegen die potenzielle Ausnutzung von Mängeln oder Schwachstellen, auf den sie ausgelegt sind, unterschieden werden. Mit den weitverbreiteten und standardisierten AVA_VAN-Stufen kann ein solcher Grad der Widerstandsfähigkeit angegeben werden. Die AVA_VAN-Stufen sind in den öffentlich zugänglichen Normen für Gemeinsame Kriterien und die Gemeinsame Evaluierungsmethodik festgelegt, die den bestehenden, auf dem Markt weitverbreiteten Zertifizierungsrahmen, wie der Durchführungsverordnung (EU) 2024/482 der Kommission ([3]), unterliegen. Mit der

([3]) Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC) (ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

Durchführungsverordnung (EU) 2024/482 wurde ein europäisches System für die Cybersicherheitszertifizierung eingeführt, das zur Zertifizierung eines Produkts unter Angabe bestimmter Vertrauenswürdigkeitsstufen verwendet werden kann. Gestützt auf weltweite Praktiken sieht die Durchführungsverordnung (EU) 2024/482 die Möglichkeit vor, bis Ende 2027 Zertifikate auf der Grundlage früherer Versionen der Normen auszustellen. Im Zusammenhang mit der Verordnung (EU) 2024/2847 sollte es daher zulässig sein, die AVA_VAN-Stufen durch Bezugnahme auf die neueste Version oder auf frühere Versionen dieser Normen auszudrücken.

(9) Die in dieser Verordnung vorgesehenen Maßnahmen stehen im Einklang mit der Stellungnahme des nach Artikel 62 Absatz 1 der Verordnung (EU) 2024/2847 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Gemeinsame Kriterien“ die Gemeinsamen Kriterien für die Evaluierung der IT-Sicherheit im Sinne von Artikel 2 Absatz 1 der Durchführungsverordnung (EU) 2024/482 oder gemäß den in Artikel 3 Absatz 2 Buchstaben a und b jener Durchführungsverordnung genannten Normen;
2. „Gemeinsame Evaluierungsmethodik“ die Gemeinsame Methodik für die Evaluierung der IT-Sicherheit im Sinne von Artikel 2 Absatz 2 der Durchführungsverordnung (EU) 2024/482 oder gemäß den in Artikel 3 Absatz 2 Buchstaben c und d jener Durchführungsverordnung genannten Normen.

Artikel 2

(1) Die technische Beschreibung der nach Anhang III der Verordnung (EU) 2024/2847 zu den Klassen I und II gehörigen Kategorien von Produkten mit digitalen Elementen ist in Anhang I der vorliegenden Verordnung festgelegt.

(2) Die technische Beschreibung der Kategorien von Produkten mit digitalen Elementen gemäß Anhang IV der Verordnung (EU) 2024/2847 ist in Anhang II der vorliegenden Verordnung festgelegt.

Artikel 3

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 28. November 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG I

WICHTIGE PRODUKTE MIT DIGITALEN ELEMENTEN

Klasse I

Produktkategorie	Technische Beschreibung
1. Identitätsmanagementsysteme sowie Software und Hardware für die Verwaltung privilegierter Zugänge, einschließlich Lesegeräte für die Authentifizierung und Zugangskontrolle, auch biometrische Lesegeräte	Identitätsmanagementsysteme sind Produkte mit digitalen Elementen, die Mechanismen für die Authentifizierung oder Autorisierung bieten wie auch Mechanismen für das Lebenszyklusmanagement von Identitätsnachweisen natürlicher Personen, juristischer Personen, von Geräten oder Systemen, wie etwa Identitätsregistrierung, -bereitstellung, -pflege und Streichung von Registrierungsdaten, bieten können. Zu diesen Systemen gehören Zugangsverwaltungssysteme, die den Zugang für natürliche Personen, juristische Personen, Geräte oder Systeme zu digitalen Ressourcen oder physischen Standorten kontrollieren. Software für die Verwaltung privilegierter Zugänge ist ein Zugangsverwaltungssystem, das die Zugangsrechte zu IT- oder OT-Systemen und sensiblen Informationen innerhalb einer Organisation kontrolliert und überwacht, einschließlich Systemen zur Durchsetzung differenzierter Zugangskontrollkonzepte für privilegierte Nutzer. Zu dieser Kategorie gehören unter anderem Lesegeräte für die Authentifizierung und Zugangskontrolle, biometrische Lesegeräte, Single-Sign-On-Software, föderierte Identitätsmanagementsoftware, Einmalpasswort-Software, Hardware-Authentifizierungsgeräte wie Generatoren für Transaktionsnummern (TAN-Generatoren), Authentifizierungssoftware und Multi-Faktor-Authentifizierungssoftware.
2. eigenständige und eingebettete Browser	Softwareprodukte mit digitalen Elementen, die es Endnutzern ermöglichen, auf Webinhalte und -dienste zuzugreifen, diese bereitzustellen und zu nutzen, die auf Servern gehostet werden, welche mit Netzwerken wie beispielsweise dem Internet verbunden sind. Sie umfassen üblicherweise eine Browser-Engine für die Interpretation und das Anzeigen von Inhalten in Auszeichnungssprachen (z. B. HTML), die Unterstützung von Netzwerkprotokollen (z. B. HTTP, HTTPS), die Fähigkeit zur Ausführung von Skripten und zur Verwaltung von Nutzereingaben sowie die Speicherung vorübergehender oder dauerhafter Daten von Websites (Cookies). Diese Kategorie umfasst unter anderem eigenständige Anwendungen, die die Funktionen von Browsern erfüllen, eingebettete Browser, die für die Integration in ein anderes System oder eine andere Anwendung bestimmt sind, sowie Browser mit integrierten KI-Agenten.
3. Passwort-Manager	Produkte mit digitalen Elementen, die Passwörter lokal auf einem Gerät oder auf einem entfernten Server speichern, einschließlich Tätigkeiten wie der Generierung von Passwörtern sowie der gemeinsamen Nutzung von Passwörtern und der Integration in lokale Anwendungen oder Anwendungen Dritter für die Nutzung von Passwörtern. Diese Kategorie umfasst unter anderem lokale Passwort-Manager, Passwort-Manager, die als Browser-Erweiterungen bereitgestellt werden, Passwort-Manager für Unternehmen sowie hardwarebasierte Passwort-Manager.

Produktkategorie	Technische Beschreibung
4. Software für die Suche, Entfernung und Quarantäne von Schadsoftware	Softwareprodukte mit digitalen Elementen, üblicherweise als Antiviren- oder Anti-Malware-Software bezeichnet, die Schadsoftware oder -codes auf Geräten erkennen oder suchen oder diese Software oder diese Codes entfernen oder unter Quarantäne stellen, um die Integrität, Vertraulichkeit oder Verfügbarkeit solcher Geräte zu wahren. Im Zusammenhang mit dieser Produktkategorie bezeichnet Schadsoftware eine Software, die bösartige Merkmale oder Fähigkeiten aufweist, die dem Nutzer und/oder dem Computersystem direkt oder indirekt Schaden zufügen können wie etwa Viren, Würmer, Ransomware, Spähsoftware und Trojaner. Zu dieser Kategorie gehört unter anderem Software, die Schadsoftware in Echtzeit oder manuell aufspürt oder sucht, sowie Rootkit-Aufspür-Software und Notfall-CD-Software mit der Kernfunktion, Schadsoftware zu suchen, zu entfernen oder in Quarantäne zu stellen.
5. Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzes (VPN)	Produkte mit digitalen Elementen, die einen logischen verschlüsselten Tunnel einrichten, der aus den Systemressourcen eines physischen oder virtuellen Netzes hergestellt wird. Zu dieser Kategorie gehören unter anderem VPN-Clients, VPN-Server und VPN-Gateways.
6. Netzmanagementsysteme	Produkte mit digitalen Elementen, die verbundene Netzkomponenten wie Server, Router, Switches, Arbeitsplatzrechner, Drucker oder mobile Geräte verwalten, indem sie sie überwachen und ihren Netzbetrieb und ihre Konfiguration kontrollieren. Diese Kategorie umfasst unter anderem Ende-zu-Ende-Managementsysteme und spezielle Konfigurationsmanagementsysteme wie etwa Controller für softwaredefinierte Netzwerke.
7. Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)	Produkte mit digitalen Elementen, die Daten aus verschiedenen Quellen erheben, diese Daten analysieren und in Korrelation setzen und sie zu sicherheitsrelevanten Zwecken, etwa zur Erkennung von Bedrohungen und Vorfällen, zur forensischen Analyse oder hinsichtlich der Einhaltung von Vorschriften, als verwertbare Informationen bereitstellen.
8. Bootmanager	Softwareprodukte mit digitalen Elementen, die den Vorgang des Systemstarts nach dem Einschalten/Neustart des Systems steuern, indem sie die Hardware initialisieren, die Betriebssystemumgebung oder Systemressourcen laden bzw. die Steuerung an diese abgeben und Bootoptionen auswählen. Zu dieser Kategorie gehören unter anderem UEFI-Firmware oder einstufige und mehrstufige Bootloader.
9. Public-Key-Infrastrukturen und Software für die Ausstellung digitaler Zertifikate	Produkte mit digitalen Elementen, die als Teil einer Public-Key-Infrastruktur (PKI) verwendet werden und die die Validierung, Erstellung, Ausstellung, Verbreitung, den Stand der Veröffentlichung, die Erneuerung oder den Widerruf digitaler Zertifikate oder die Erzeugung, Speicherung, Hinterlegung, den Austausch, die Vernichtung oder Rotation von kryptografischen Schlüsseln, die mit solchen digitalen Zertifikaten verbunden sind, verwalten. Diese Kategorie umfasst unter anderem Schlüsselmanagementsysteme, Managementsysteme für digitale Zertifikate, Online Certificate Status Protocol Responder und ganzheitliche PKI-Lösungen.

Produktkategorie	Technische Beschreibung
10. physische und virtuelle Netzschnittstellen	Physische Netzschnittstellen sind Produkte mit digitalen Elementen, die ein Gerät über eine von den Schnittstellentreibern – die üblicherweise Teil der Sicherungsschicht sind – bereitgestellte Anwendungsprogrammierschnittstelle (API) direkt mit einem Netz verbinden, und verfügen über Hardware-Adapter zu den Übertragungsmedien mit entsprechender Firmware – die üblicherweise Teil der Bitübertragungsschicht und der Sicherungsschicht sind. Virtuelle Netzschnittstellen sind Produkte mit digitalen Elementen, die ein Gerät direkt oder indirekt über eine API mit einem Netz verbinden, wobei diese API die von Treibern physischer Netzschnittstellen bereitgestellte Schnittstelle emuliert, die üblicherweise Teil der Sicherungsschicht sind. Diese Kategorie umfasst unter anderem drahtgebundene und drahtlose Netzschnittstellenkarten, Controller und Adapter wie WLAN, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee oder Feldbus sowie rein virtuelle eigenständige Produkte wie virtuelle Netzschnittstellenkarten, Container-Netzschnittstellen und VPN-Schnittstellen.
11. Betriebssysteme	Softwareprodukte mit digitalen Elementen, die eine abstrakte Schnittstelle der zugrunde liegenden Hardware bereitstellen und die Ausführung von Software steuern und Dienste wie Rechenressourcenmanagement und -konfiguration, Planung, Ein-Ausgabe-Steuerung, Datenverwaltung und Bereitstellung einer Schnittstelle für die Interaktion von Anwendungen mit Systemressourcen und Peripheriegeräten erbringen können. Zu dieser Kategorie gehören unter anderem Echtzeit-Betriebssysteme, allgemeine und spezielle Betriebssysteme.
12. Router, Modems für die Internetanbindung und Switches	Router sind Produkte mit digitalen Elementen, die den Datenfluss zwischen verschiedenen Netzen durch die Auswahl von Pfaden oder Routen unter Verwendung von Routingprotokoll-Mechanismen und -Algorithmen ermöglichen und steuern und üblicherweise Teil der Vermittlungsschicht sind. Zu dieser Kategorie gehören unter anderem drahtgebundene und drahtlose Router, virtuelle Router und Router mit oder ohne Modems.
	Modems für die Internetanbindung sind Hardwareprodukte mit digitalen Elementen, die digitale Modulations- und Demodulationsverfahren verwenden, um analoge Signale von digitalen Signalen und in digitale Signale für die IP-gestützte Kommunikation umzuwandeln. Zu dieser Kategorie gehören unter anderem Glasfasermodems, DSL-Modems, Kabelmodems (DOCSIS), Satellitenmodems und zellulare Modems.
	Switches sind Produkte mit digitalen Elementen, die die Konnektivität zwischen vernetzten Geräten durch Paketweiterleitungsmechanismen ermöglichen, über eine Managementebene verfügen und die üblicherweise Teil der Sicherungsschicht oder der Vermittlungsschicht sind. Diese Kategorie umfasst unter anderem Managed Switches, Smart Switches, Multilayer Switches, Virtual Security Switches, programmierbare Switches für softwaredefinierte Netzwerke und Bridges wie etwa drahtlose Zugangspunkte.

Produktkategorie	Technische Beschreibung
13. Mikroprozessoren mit sicherheitsrelevanten Funktionen	Produkte mit digitalen Elementen, bei denen es sich um integrierte Schaltungen handelt, die als Hauptprozessor fungieren und externer Speicher und Peripheriegeräten bedürfen, einschließlich Mikrocode und anderer Low-Level-Firmware. Darüber hinaus stellen sie sicherheitsrelevante Funktionen wie Verschlüsselung, Authentifizierung, sichere Schlüsselspeicherung, Zufallszahlengenerierung, vertrauenswürdige Ausführungsumgebung oder andere hardwarebasierte Sicherheitsmechanismen bereit, die darauf abzielen, andere Produkte, Netze oder Dienste neben dem Mikroprozessor selbst zu sichern, wie etwa eine sichere Boot Chain, Virtualisierung oder sichere Kommunikationsschnittstellen.
14. Mikrocontroller mit sicherheitsrelevanten Funktionen	Produkte mit digitalen Elementen, bei denen es sich um integrierte Schaltungen handelt, die als Hauptprozessor fungieren und einen Speicher integrieren, wodurch der Mikrocontroller programmierbar wird, sowie um andere Peripheriegeräte, einschließlich Mikrocode und anderer Low-Level-Firmware. Darüber hinaus stellen sie sicherheitsrelevante Funktionen wie Verschlüsselung, Authentifizierung, sichere Schlüsselspeicherung, Zufallszahlengenerierung, vertrauenswürdige Ausführungsumgebung oder andere hardwarebasierte Sicherheitsmechanismen bereit, die darauf abzielen, andere Produkte, Netze oder Dienste neben dem Mikrocontroller selbst zu sichern, wie etwa sichere Bootketten, Virtualisierung oder sichere Kommunikationsschnittstellen.
15. anwendungsspezifische integrierte Schaltungen (ASIC) und FPGA (Field Programmable Gate Array) mit sicherheitsrelevanten Funktionen	Anwendungsspezifische integrierte Schaltungen (ASIC) mit sicherheitsrelevanten Funktionen sind Produkte mit digitalen Elementen, bei denen es sich um integrierte Schaltungen handelt, die vollständig oder teilweise maßgeschneidert sind und dazu konzipiert wurden, eine bestimmte Funktion auszuführen oder eine bestimmte Anwendung zu implementieren, einschließlich Mikrocode und anderer Low-Level-Firmware. Darüber hinaus stellen sie sicherheitsrelevante Funktionen wie Verschlüsselung, Authentifizierung, sichere Schlüsselspeicherung, Zufallszahlengenerierung, vertrauenswürdige Ausführungsumgebung oder andere hardwarebasierte Sicherheitsmechanismen bereit, die darauf abzielen, andere Produkte, Netze oder Dienste neben den ASIC selbst zu sichern, wie etwa sichere Bootketten, Virtualisierung oder sichere Kommunikationsschnittstellen.
	FPGAs (Field Programmable Gate Arrays) mit sicherheitsrelevanten Funktionen sind Produkte mit digitalen Elementen, bei denen es sich um integrierte Schaltungen handelt, die durch eine Matrix konfigurierbarer Logikblöcke gekennzeichnet sind und nach der Herstellung zur Ausführung einer bestimmten Funktion oder zur Implementierung einer bestimmten Anwendung reprogrammierbar sind, einschließlich Mikrocode und anderer Low-Level-Firmware. Darüber hinaus stellen sie sicherheitsrelevante Funktionen wie Verschlüsselung, Authentifizierung, sichere Schlüsselspeicherung, Zufallszahlengenerierung, vertrauenswürdige Ausführungsumgebung oder andere hardwarebasierte Sicherheitsmechanismen bereit, die darauf abzielen, andere Produkte, Netze oder Dienste neben den FPGAs selbst zu sichern, wie etwa sichere Bootketten, Virtualisierung oder sichere Kommunikationsschnittstellen.
16. virtuelle Assistenten für die intelligente häusliche Umgebung mit allgemeinem Zweck	Produkte mit digitalen Elementen, die – direkt oder über andere Geräte – via öffentliches Internet kommunizieren, die Anforderungen, Aufgaben oder Fragen auf der Grundlage natürlicher Sprache bearbeiten, etwa durch Audio- oder schriftliche Eingaben, und die auf der Grundlage dieser Anforderungen, Aufgaben oder Fragen Zugang zu anderen Diensten gewähren oder die Funktionen vernetzter Geräte in Wohnumgebungen steuern. Diese Kategorie umfasst unter anderem intelligente Lautsprecher mit einem integrierten virtuellen Assistenten und eigenständige virtuelle Assistenten, die dieser Beschreibung entsprechen.

Produktkategorie	Technische Beschreibung
17. Produkte für die intelligente häusliche Umgebung mit Sicherheitsfunktionen, einschließlich intelligenter Türschlösser, Sicherheitskameras, Babyüberwachungssysteme und Alarmanlagen	Produkte mit digitalen Elementen, die die physische Sicherheit von Verbrauchern in einer Wohnumgebung schützen und die von anderen Systemen ferngesteuert oder aus der Ferne verwaltet werden können, sowie Hardware und Software, die die zentrale Steuerung solcher Produkte ermöglichen. Zu dieser Kategorie gehören unter anderem intelligente Türschlösser, Babyüberwachungssysteme, Alarmanlagen und Heimüberwachungskameras.
18. mit dem Internet verbundenes Spielzeug, das unter die Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates ([1]) fällt und über Funktionen zur sozialen Interaktion (z. B. sprechen oder filmen) oder zur Ortung verfügt	Mit dem Internet verbundenes Spielzeug, das über Funktionen zur sozialen Interaktion verfügt, sind Produkte mit digitalen Elementen, die unter die Richtlinie 2009/48/EG fallen, via öffentliches Internet – direkt oder über andere Geräte – kommunizieren und über eingebettete Technologien verfügen, die eine eingehende und ausgehende Kommunikation ermöglichen, wie etwa Tastatur, Mikrofon, Lautsprecher oder Kamera.
	Mit dem Internet verbundenes Spielzeug, das über Funktionen zur Ortung verfügt, sind Produkte mit digitalen Elementen, die unter die Richtlinie 2009/48/EG fallen, via öffentliches Internet – direkt oder über andere Geräte – kommunizieren und über Technologien verfügen, die die Ortung oder Rückschlüsse auf geografische Standorte von Spielzeugen oder deren Benutzer ermöglichen. Wenn das Spielzeug lediglich die Nähe des Benutzers oder anderer Spielzeuge mittels Sensortechnik erkennt, gilt es nicht als mit Ortungsfunktionen ausgestattet.
19. am Körper tragbare Produkte, die zum Zwecke der Gesundheitsüberwachung (z. B. Tracking) bestimmt sind und nicht unter die Verordnung (EU) 2017/745 ([2]) oder (EU) 2017/746 des Europäischen Parlaments und des Rates ([3]) fallen, oder am Körper tragbare Produkte, die für die Verwendung durch und für Kinder bestimmt sind	Am Körper tragbare Produkte, die zum Zwecke der Gesundheitsüberwachung bestimmt sind, sind Produkte mit digitalen Elementen, die direkt oder über Kleidung oder Accessoires am Körper getragen werden und regelmäßig oder kontinuierlich Informationen, einschließlich Körpermessdaten, die für die Gesundheit des Nutzers relevant sind, erfassen und weiterverarbeiten können, und die nicht unter die Verordnung (EU) 2017/745 oder die Verordnung (EU) 2017/746 fallen. Diese Kategorie umfasst unter anderem Fitness-Tracker, Smartwatches, intelligenten Schmuck, intelligente Kleidung und intelligente Sportbekleidung, die dieser Beschreibung entsprechen.
	Am Körper tragbare Produkte, die von Kindern verwendet werden oder für diese bestimmt sind, sind Produkte mit digitalen Elementen, die direkt oder über Kleidung oder Accessoires von Personen unter 14 Jahren getragen oder am Körper angebracht werden können. Zu dieser Kategorie gehören unter anderem am Körper getragene Produkte für die Sicherheit von Kindern.

([1]) Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Sicherheit von Spielzeug (ABl. L 170 vom 30.6.2009, S. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Klasse II

Produktkategorie	Technische Beschreibung
1. Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen	Hypervisoren sind Softwareprodukte mit digitalen Elementen, die Rechenressourcen abstrahieren und/oder zuweisen und die Ausführung, Verwaltung und Orchestrierung virtueller Maschinen ermöglichen, die logisch voneinander und/oder von der physischen Hardware getrennt sind. Hypervisoren können direkt auf Hardware (Bare Metal), auf einem Betriebssystem oder innerhalb einer anderen virtuellen Maschine (geschachtelte Virtualisierung) betrieben werden. Im Zusammenhang mit dieser Produktkategorie ist eine virtuelle Maschine eine softwaredefinierte logische Trennung einer Rechenumgebung, die virtuelle Hardware-Ressourcen (z. B. CPU, Arbeitsspeicher, Speicher, Netzschnittstellen) umfasst und üblicherweise über ein eigenes Betriebssystem verfügt. Zu dieser Kategorie gehören unter anderem Typ-1-Hypervisoren (Bare Metal), Typ-2-Hypervisoren (in einem Betriebssystem gehostet) und Hybrid-Hypervisoren.
	Container-Runtime-Systeme sind Softwareprodukte mit digitalen Elementen, die die Ausführung und den Lebenszyklus von Containern, die über ein einziges Host-Betriebssystem laufen, als isolierte Prozesse steuern, Ressourcen zuweisen und die Verwaltung und Orchestrierung einzelner Container ermöglichen. Im Zusammenhang mit dieser Produktkategorie ist ein Container eine softwaregestützte Ausführungsumgebung, in der eine oder mehrere Softwarekomponenten und deren Abhängigkeiten in einem einzigen Paket zusammengefasst sind, sodass sie unabhängig und einheitlich ausgeführt werden können.
2. Firewalls, Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme	Firewalls sind Produkte mit digitalen Elementen, die ein verbundenes Netz oder System vor unbefugtem Zugriff schützen, indem sie den ein- und ausgehenden Datenverkehr dieses Netzes überwachen und einschränken. Zu dieser Kategorie gehören unter anderem Netzwerk-Firewalls und Anwendungs-Firewalls (wie etwa Webanwendungs-Firewalls) oder Filter und Anti-Spam-Gateways.
	Intrusion-Detection-Systeme sind Produkte mit digitalen Elementen, die den Datenverkehr nach dessen Eintritt in die Netzwerkumgebung auf verdächtige Aktivität überwachen und erkennen oder feststellen, ob ein Angriff auf ein verbundenes Netz oder System versucht wurde, stattfindet oder stattgefunden hat. Zu dieser Kategorie gehören unter anderem netzgestützte Intrusion-Detection-Systeme und hostbasierte Intrusion-Detection-Systeme.
	Intrusion-Prevention-Systeme sind Produkte mit digitalen Elementen, die aus einem Intrusion-Detection-System bestehen, das aktiv auf einen Angriff auf ein verbundenes Netz oder System reagiert. Zu dieser Kategorie gehören unter anderem netzgestützte Intrusion-Prevention-Systeme und hostbasierte Intrusion-Prevention-Systeme.

Produktkategorie	Technische Beschreibung
3. manipulationssichere Mikroprozessoren	Produkte mit digitalen Elementen, bei denen es sich um Mikroprozessoren mit sicherheitsrelevanten Funktionen, wie etwa Manipulationserkennung, -widerstandsfähigkeit oder -reaktion, gemäß Klasse I Nummer 13 des vorliegenden Anhangs handelt und die zusätzlich so konzipiert sind, dass sie den Schutz gemäß AVA_VAN-Stufe 2 oder 3 bieten, wie in den Gemeinsamen Kriterien und der Gemeinsamen Evaluierungsmethodik festgelegt.
4. manipulationssichere Mikrocontroller	Produkte mit digitalen Elementen, bei denen es sich um Mikrocontroller mit sicherheitsrelevanten Funktionen, wie etwa Manipulationserkennung, -widerstandsfähigkeit oder -reaktion, gemäß Klasse I Nummer 14 des vorliegenden Anhangs handelt und die zusätzlich so konzipiert sind, dass sie Schutz gemäß AVA_VAN-Stufe 2 oder 3 bieten, wie in den Gemeinsamen Kriterien und der Gemeinsamen Evaluierungsmethodik festgelegt.

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

ANHANG II

KRITISCHE PRODUKTE MIT DIGITALEN ELEMENTEN

Produktkategorie	Technische Beschreibung
1. Hardwaregeräte mit Sicherheitsboxen	Hardwareprodukte mit digitalen Elementen, die sensible Daten sicher speichern, verarbeiten oder verwalten oder kryptografische Vorgänge ausführen, aus mehreren diskreten Bauelementen bestehen, über eine physische Hardwarehülle verfügen und Manipulationserkennung, -widerstandsfähigkeit oder -reaktion als Abwehrmittel gegen physische Angriffe bieten. Zu dieser Kategorie gehören unter anderem physische Zahlungsterminals, Hardware-Sicherheitsmodule, die kryptografische Elemente erzeugen und verwalten, sowie Fahrtenschreiber, die der vorstehenden Beschreibung entsprechen.
2. Smart-Meter-Gateways in intelligenten Messsystemen im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates ([1]) sowie andere Geräte für fortgeschrittene Sicherheitszwecke, einschließlich der sicheren Kryptoverarbeitung	Smart-Meter-Gateways sind Produkte mit digitalen Elementen, die die Kommunikation zwischen Komponenten in intelligenten Messsystemen (im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944) oder an diese angeschlossenen Komponenten und befugten Dritten wie Versorgungsunternehmen steuern. Smart-Meter-Gateways erfassen, verarbeiten und speichern Messdaten oder personenbezogene Daten, schützen Daten- und Informationsflüsse durch Unterstützung spezifischer kryptografischer Anforderungen wie Verschlüsselung und Entschlüsselung von Daten, umfassen Firewall-Funktionen und stellen Hilfsmittel zur Steuerung anderer Geräte bereit. Diese Kategorie umfasst unter anderem Smart-Meter-Gateways im Zusammenhang mit intelligenten Messsystemen zur Messung von Elektrizität im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944. Sie kann auch intelligente Smart-Meter-Gateways umfassen, die im Rahmen anderer intelligenter Messsysteme zur Messung des Verbrauchs anderer Energiequellen wie Gas oder Wärme verwendet werden, sofern das Gateway dieser Beschreibung entspricht.
3. Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselemente	Sicherheitselemente sind Mikrocontroller oder Mikroprozessoren mit sicherheitsrelevanten Funktionen wie etwa Manipulationserkennung, -widerstandsfähigkeit oder -reaktion. Sie speichern, verarbeiten oder verwalten üblicherweise kryptografische Vorgänge oder sensible Daten wie Identitätsnachweise oder Zahlungsdaten. Sicherheitselemente sind so konzipiert, dass sie Schutz mindestens auf AVA_VAN-Stufe 4 bieten, wie in den Gemeinsamen Kriterien oder der Gemeinsamen Evaluierungsmethodik festgelegt. Sie können diskrete Bauelemente aus Silizium sein oder in Ein-Chip-Systeme (System-on-a-Chip, SoC) integriert werden. Sicherheitselemente können eine Anwendungsumgebung oder ein Betriebssystem sowie eine oder mehrere Anwendungen umfassen. Zu dieser Kategorie gehören unter anderem Trusted Platform Modules (TPMs) und die embedded Universal Integrated Circuit Card (eUICC).
	Chipkarten oder ähnliche Geräte sind Sicherheitselemente, die in ein Trägermaterial wie etwa Kunststoff oder Holz in Form einer Karte integriert sind, oder Sicherheitselemente, die in Trägermaterialien in anderer Form integriert sind. Zu dieser Kategorie gehören unter anderem Ausweis- und Reisedokumente, qualifizierte Signaturkarten, austauschbare UICCs, physische Zahlungskarten, physische Zugangskarten, Karten für digitale Fahrtenschreiber oder Armbänder mit integrierten Sicherheitselementen für Zahlungen.

([1]) Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU (ABl. L 158 vom 14.6.2019, S. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).