2025/2392

1.12.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/2392

af 28. november 2025

om den tekniske beskrivelse af kategorierne af vigtige og kritiske produkter med digitale elementer i henhold til Europa-Parlamentets og Rådets forordning (EU) 2024/2847

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) ([1]), særlig artikel 7, stk. 4, og

ud fra følgende betragtninger:

(1) Forordning (EU) 2024/2847 fastsætter cybersikkerhedsregler for produkter med digitale elementer. Bilag III til nævnte forordning fastsætter navnlig kategorierne af vigtige produkter med digitale elementer, der, når de bringes i omsætning, er underlagt strengere procedurer for overensstemmelsesvurdering end dem, der gælder for andre produkter med digitale elementer. Bilag IV til forordning (EU) 2024/2847 fastsætter kategorierne af kritiske produkter med digitale elementer, for hvilke fabrikanter kan pålægges at indhente en europæisk cybersikkerhedsattest i henhold til en europæisk cybersikkerhedscertificeringsordning i henhold til Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([2]), eller som vil være underlagt en obligatorisk tredjepartsoverensstemmelsesvurdering, når de bringes i omsætning.

(2) I henhold til artikel 7, stk. 1, og artikel 8, stk. 1, i forordning (EU) 2024/2847 afgør den væsentligste funktionalitet af et produkt med digitale elementer, om det pågældende produkt med digitale elementer svarer til den tekniske beskrivelse af en kategori af vigtige eller kritiske produkter med digitale elementer og dermed de gældende overensstemmelsesvurderingsprocedurer.

(3) Ved udviklingen af et produkt med digitale elementer og for at opnå de ønskede funktioner integrerer fabrikanterne typisk andre komponenter, som også er produkter med digitale elementer, i deres egne produkter med digitale elementer, hvor disse andre komponenter kan svare til den tekniske beskrivelse af en kategori af vigtige eller kritiske produkter. I henhold til forordning (EU) 2024/2847 er et produkt med digitale elementer omfattet af de overensstemmelsesvurderingsprocedurer, der gælder for vigtige eller kritiske produkter med digitale elementer, hvis produktet som helhed er et vigtigt eller kritisk produkt som fastsat i bilag III og IV til nævnte forordning. For eksempel medfører integration af en indlejret browser som en komponent i en nyhedsapplikation til smartphones ikke i sig selv, at nyhedsapplikationen er omfattet af den overensstemmelsesvurderingsprocedure, der gælder for produkter med digitale elementer med den væsentlige funktionalitet »enkeltstående og indlejrede browsere«. Ikke desto mindre skal fabrikanten i overensstemmelse med forordning (EU) 2024/2847 sikre, at produktet med digitale elementer som helhed opfylder de væsentlige cybersikkerhedskrav. Fabrikanten skal derfor evaluere sikkerheden af hele produktet under hensyntagen til, hvor det er relevant, sikkerheden af de komponenter eller funktioner, der er integreret i det. I eksemplet med en producent af en nyhedsapplikation, hvor denne skal påvise, at produktet med digitale elementer er i overensstemmelse med forordning (EU) 2024/2847, skal det påvises, at nyhedsapplikationen som helhed opfylder de gældende krav, idet der, hvor det er relevant, tages hensyn til sikkerheden af den indlejrede browser, der er integreret i applikationen.

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

([2]) Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Det forhold, at et produkt med digitale elementer udfører andre funktioner end eller ud over dem, der er omfattet af de tekniske beskrivelser i denne forordning, betyder ikke i sig selv, at produktet med digitale elementer ikke har en væsentlig funktionalitet, der hører ind under en produktkategori, der er fastsat i bilag III og IV til forordning (EU) 2024/2847. For eksempel omfatter produkter med digitale elementer, der har den væsentligste funktionalitet »operativsystemer«, ofte software, der udfører accessoriske funktioner, der ikke er medtaget i den tekniske beskrivelse af den pågældende produktkategori, såsom en regnemaskine eller en simpel grafikeditor. Produkter med digitale elementer indeholder ofte også komponenter, der har samme funktionalitet som et andet vigtigt eller kritisk produkt med digitale elementer, såsom et operativsystem, der integrerer browserfunktioner, eller en router, der integrerer firewall-funktionaliteten. Dette betyder imidlertid ikke i sig selv, at sådanne produkter med digitale elementer ikke har som væsentligste funktionalitet henholdsvis »operativsystemer« eller »routere, modemmer til internetforbindelse og afbrydere«.

(5) På den anden side skal et produkt med digitale elementer, der er i stand til at udføre funktionerne i en produktkategori, der er fastsat i bilag III og IV til forordning (EU) 2024/2847, men hvis væsentligste funktionalitet i sig selv er forskellig fra funktionaliteten for en sådan produktkategori, ikke anses for at svare til den tekniske beskrivelse af den pågældende produktkategori. For eksempel er software til sikkerhedsorganisering, -automatisering og -reaktion (SOAR) ofte i stand til at udføre de samme funktioner som produkter med digitale elementer i kategorien »systemer til sikkerhedsinformations- og hændelseshåndtering (SIEM)«, dvs. indsamle data, analysere dem og præsentere dem som anvendelige oplysninger til sikkerhedsformål. Da SOAR-softwarens væsentligste funktionalitet imidlertid ikke er den samme som SIEM-systemets, skal den generelt ikke anses for at svare til den tekniske beskrivelse af »systemer til sikkerhedsinformations- og hændelseshåndtering (SIEM)«. På samme måde integrerer en smartphone typisk komponenter, der udfører funktioner, som svarer til flere af de produktkategorier, der er fastsat i bilag III og IV til forordning (EU) 2024/2847, såsom et operativsystem eller en integreret adgangskodeadministrator. Men eftersom en smartphones væsentligste funktionalitet ikke omfatter et operativsystem eller en adgangskodeadministrator, skal den generelt ikke anses for at svare til den tekniske beskrivelse af sådanne produktkategorier.

(6) I henhold til artikel 13, stk. 2 og 3, i forordning (EU) 2024/2847 skal fabrikanter af produkter med digitale elementer gennemføre de væsentlige cybersikkerhedskrav, der er fastsat i del I i bilag I til forordning (EU) 2024/2847, på en måde, der står i et rimeligt forhold til risiciene ved produktet med digitale elementer, baseret på det tilsigtede formål og den anvendelse, der med rimelighed kan forudses, samt betingelserne for anvendelse af produktet med digitale elementer, idet der tages højde for, hvor længe produktet forventes at være i brug. I overensstemmelse med nævnte forordnings artikel 13, stk. 2 og 3, og uanset om produktet med digitale elementer anses for at være et vigtigt eller kritisk produkt med digitale elementer, skal fabrikanterne foretage en omfattende cybersikkerhedsrisikovurdering og angive, hvordan de væsentlige cybersikkerhedskrav gennemføres på grundlag af risikovurderingen, herunder deres test og sikkerhed. Hvis den væsentligste funktionalitet i fabrikantens produkt med digitale elementer svarer til den tekniske beskrivelse af et vigtigt eller kritisk produkt med digitale elementer, skal fabrikanten påvise overensstemmelse efter de specifikke overensstemmelsesvurderingsprocedurer, der er fastsat i artikel 32, stk. 2-5 i forordning (EU) 2024/2847.

(7) Denne forordning indeholder eksempler på produkter med digitale elementer, hvis væsentligste funktionalitet svarer til den tekniske beskrivelse af visse vigtige eller kritiske produkter med digitale elementer. Disse eksempler er kun til illustrative formål og udgør ikke en udtømmende liste.

(8) For at skabe retssikkerhed for fabrikanterne bør der skelnes mellem kategorierne af produkter med digitale elementer »mikroprocessorer, der er sikret mod manipulation«, »mikrocontrollere, der er sikret mod manipulation« og »smartcards eller lignende enheder, herunder sikre elementer« på grundlag af det niveau af potentiel udnyttelse af fejl eller svagheder, som de er designet til at kunne modstå. AVA_VAN-niveauer er en udbredt og standardiseret måde at udtrykke et sådant modstandsdygtighedsniveau på. AVA_VAN-niveauerne er defineret i de offentligt tilgængelige standarder for fælles kriterier og fælles evalueringsmetoder, som udgør grundlaget for de eksisterende certificeringsrammer, der i vid udstrækning anvendes på markedet, såsom Kommissionens gennemførelsesforordning

(EU) 2024/482 ([3]). Ved gennemførelsesforordning (EU) 2024/482 blev der oprettet en europæisk cybersikkerhedscertificeringsordning, som kan anvendes til at påvise et produkts overensstemmelse med et specifikt tillidsniveau. I overensstemmelse med global praksis giver gennemførelsesforordning (EU) 2024/482 mulighed for at udstede certifikater på grundlag af ældre versioner af standarderne indtil udgangen af 2027. I forbindelse med forordning (EU) 2024/2847 bør det derfor tillades, at AVA_VAN-niveauer udtrykkes med henvisning til den nyeste version eller tidligere versioner af disse standarder.

(9) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 62, stk. 1, i forordning (EU) 2024/2847 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Definitioner

I denne forordning forstås ved:

1) »fælles kriterier«: de fælles kriterier for evaluering af informationsteknologisikkerhed som defineret i artikel 2, nr. 1), i gennemførelsesforordning (EU) 2024/482 eller som fastsat i de standarder, der er omhandlet i artikel 3, stk. 2, litra a) og b), i nævnte gennemførelsesforordning

2) »fælles evalueringsmetode«: den fælles metode til evaluering af informationsteknologisikkerhed som defineret i artikel 2, nr. 2), i gennemførelsesforordning (EU) 2024/482 eller som fastsat i de standarder, der er omhandlet i artikel 3, stk. 2, litra c) og d), i nævnte gennemførelsesforordning.

Artikel 2

1. Den tekniske beskrivelse af kategorierne af produkter med digitale elementer i klasse I og II som opført i bilag III til forordning (EU) 2024/2847 er fastsat i bilag I til nærværende forordning.

2. Den tekniske beskrivelse af kategorierne af produkter med digitale elementer som opført i bilag IV til forordning (EU) 2024/2847 er fastsat i bilag II til nærværende forordning.

Artikel 3

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 28. november 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([3]) Kommissionens gennemførelsesforordning (EU) 2024/482 af 31. januar 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

BILAG I

VIGTIGE PRODUKTER MED DIGITALE ELEMENTER

Klasse I

Produktkategori	Teknisk beskrivelse
1. Software og hardware til identitetsstyringssystemer og til styring af privilegeret adgang, herunder autentificerings- og adgangskontrollæsere, herunder biometriske læsere	Identitetsstyringssystemer er produkter med digitale elementer, der indeholder mekanismer til autentificering eller tilladelse, og som også kan omfatte mekanismer til livscyklusforvaltning af identitetsoplysninger for fysiske personer, juridiske personer, enheder eller systemer såsom mekanismer til registrering, levering, vedligeholdelse og afregistrering af identitetsoplysninger. Disse systemer omfatter adgangsstyringssystemer, der styrer fysiske personers, juridiske personers, enheders eller systemers adgang til digitale ressourcer eller fysiske lokaliteter. Software til styring af privilegeret adgang er et adgangsstyringssystem, der kontrollerer og overvåger adgangsrettigheder til IT- eller OT-systemer og følsomme oplysninger inden for en organisation, herunder systemer, der håndhæver differentierede adgangskontrolpolitikker for privilegerede brugere. Denne kategori omfatter, men er ikke begrænset til, autentificerings- og adgangskontrollæsere, biometriske læsere, single sign-on-software, samlet identitetsstyringssoftware, engangskodesoftware, hardwareautentificeringsudstyr såsom transaktionsnummervisere (TAN), autentificeringssoftware og flerfaktorautentificeringssoftware.
2. Enkeltstående og indlejrede browsere	Softwareprodukter med digitale elementer, der gør det muligt for slutbrugerne at tilgå, få gengivet og interagere med webindhold og -tjenester, der hostes på servere, der er forbundet med netværk såsom internettet. De omfatter typisk et browserprogram til tolkning og visning af indhold skrevet i et mark-up-sprog (f.eks. HTML), understøttelse af webprotokoller (f.eks. HTTP, HTTPS), udførelse af scripts og forvaltning af brugerinput samt lagring af midlertidige eller persistente data fra websteder (cookies). Denne kategori omfatter, men er ikke begrænset til, enkeltstående applikationer, der fungerer som browsere, indlejrede browsere til integration i et andet system eller en anden applikation, samt browsere med integrerede AI-agenter.
3. Adgangskoder	Produkter med digitale elementer, der lagrer adgangskoder lokalt på en enhed eller på en fjernserver, herunder også indeholdende funktioner såsom generering eller deling af adgangskoder samt integration med lokale applikationer eller tredjepartsapplikationer til brug af adgangskoder. Denne kategori omfatter, men er ikke begrænset til, lokale adgangskodeadministratorer samt adgangskodeadministratorer i form af hardware, browserudvidelser og virksomhedssoftware.

Produktkategori	Teknisk beskrivelse
4. Software, der søger efter, fjerner eller sætter ondsindet software i karantæne	Softwareprodukter med digitale elementer, typisk kaldet antivirus- eller antimalware, der opdager/opsporer ondsindet software/kode på enheder, fjerner sådan software/kode eller sætter sådan software/kode i karantæne for at bevare enhedernes integritet, fortrolighed eller tilgængelighed I forbindelse med denne kategori af produkter skal der ved ondsindet software forstås software, der indeholder ondsindede funktioner eller egenskaber, der direkte eller indirekte kan forvolde skade på brugeren og/eller computersystemet, såsom virus, orme, ransomware, spyware og trojaner. Denne kategori omfatter, men er ikke begrænset til, software, der opdager eller søger efter ondsindet software i realtid eller manuelt, rootkit-detektion og genopretningsdisks med den væsentligste funktionalitet at søge efter, fjerne eller sætte ondsindet software i karantæne.
5. Produkter med digitale elementer, der fungerer som et virtuelt privat netværk (VPN)	Produkter med digitale elementer, der etablerer en krypteret logisk tunnel fra systemressourcerne i et fysisk eller virtuelt netværk. Denne kategori omfatter, men er ikke begrænset til, virtuelle private netværksklienter, virtuelle private netværksservere og virtuelle private netværksportaler.
6. Netstyringssystemer	Produkter med digitale elementer, der styrer forbundne netværkselementer såsom servere, routere, afbrydere, arbejdsstationer, printere eller mobile enheder ved at overvåge og kontrollere deres netværksdrift og -konfiguration. Denne kategori omfatter, men er ikke begrænset til, end-to-end-styringssystemer og særlige konfigurationsstyringssystemer såsom controllere til softwaredefinerede netværk.
7. Systemer til sikkerhedsinformations- og hændelseshåndtering (SIEM)	Produkter med digitale elementer, der indsamler data fra flere kilder, analyserer og korrelerer disse data og præsenterer dem som anvendelige oplysninger til sikkerhedsrelaterede formål såsom detektion af trusler og hændelser, kriminaltekniske analyser eller håndhævelse.
8. Boot managers	Softwareprodukter med digitale elementer, der styrer den indledende systemopstartsproces efter tænding/genstart ved at initialisere hardware, indlæse eller overføre kontrol til operativsystemet eller systemressourcerne og foretage boot-indstillinger. Denne kategori omfatter, men er ikke begrænset til, UEFI-firmware, enkelttrins- og flertrins-boot-loadere.
9. Public key-infrastruktur og software for udstedelse af digitale certifikater	Produkter med digitale elementer, der anvendes som en del af en public key-infrastruktur (PKI), som forvalter validering, oprettelse, udstedelse, distribution, statusrapportering, fornyelse eller tilbagekaldelse af digitale certifikater eller generering, lagring, spærring, udveksling, destruktion eller rotation af kryptografiske nøgler, der er knyttet til sådanne digitale certifikater. Denne kategori omfatter, men er ikke begrænset til, forvaltningssystemer for nøgler og digitale certifikater, status protocol-respondere for online certifikater og alt-i-én-PKI-løsninger.

Produktkategori	Teknisk beskrivelse
10. Fysiske og virtuelle netværksgrænseflader	Fysiske netværksgrænseflader er produkter med digitale elementer, der direkte forbinder en enhed til et netværk via en applikationsprogrammeringsgrænseflade (API), der leveres af grænsefladens drivere, og som typisk opererer i datalink-laget, og som omfatter hardwareadaptere til transmissionsmedier med tilsvarende firmware, der typisk opererer i det fysiske lag og datalink-laget. Virtuelle netværksgrænseflader er produkter med digitale elementer, der direkte eller indirekte forbinder en enhed til et netværk via en API, der efterligner de fysiske netværksgrænsefladers drivere, og som typisk opererer i datalink-laget. Denne kategori omfatter, men er ikke begrænset til, kablede og trådløse netværksgrænsefladekort, styreenheder og adaptere, f.eks. til wi-fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee eller Fieldbus, samt rent virtuelle enkeltstående produkter såsom virtuelle netværksgrænsefladekort, containernetværksgrænseflader og VPN-grænseflader.
11. Operativsystemer	Softwareprodukter med digitale elementer, der udgør en abstrakt grænseflade til den underliggende hardware og styrer kørslen af software, og som kan levere tjenester såsom forvaltning og konfiguration af computerressourcer, planlægning, input-output-kontrol, dataforvaltning og en grænseflade, hvorigennem applikationer interagerer med systemressourcer og perifere enheder. Denne kategori omfatter, men er ikke begrænset til, realtidsoperativsystemer, generelle operativsystemer og operativsystemer til særlige formål.
12. Routere, modemmer til internetforbindelse og afbrydere	Routere er produkter med digitale elementer, der etablerer og styrer datastrømmen mellem forskellige netværk ved at vælge veje eller ruter ved hjælp af routingprotokolmekanismer og –algoritmer, der typisk opererer i netværkslaget. Denne kategori omfatter, men er ikke begrænset til, kablede og trådløse routere, virtuelle routere og routere med eller uden modemmer.
	Modemmer til internetforbindelse er hardwareprodukter med digitale elementer, der anvender digitale moduleringss- og demoduleringsteknikker til at konvertere mellem analoge og digitale signaler til IP-baseret kommunikation. Denne kategori omfatter, men er ikke begrænset til, fibermodemmer, DSL-modemmer (Digital Subscriber Line), kabelmodemmer (DOCSIS), satellitmodemmer og mobilmodemmer.
	Afbrydere er produkter med digitale elementer, der sikrer konnektivitet mellem netværksforbundne enheder gennem mekanismer til forwarding af datapakker, og som har et styringselement, der typisk implementeres i datalink- eller netværkslaget. Denne kategori omfatter, men er ikke begrænset til, styrede afbrydere, intelligente afbrydere, flerlagsafbrydere, virtuelle sikkerhedsafbrydere, programmerbare afbrydere til softwaredefinerede netværk og broer såsom trådløse adgangspunkter.

Produktkategori	Teknisk beskrivelse
13. Mikroprocessorer med sikkerhedsrelaterede funktioner	Produkter med digitale elementer, som er integrerede kredsløb, der udfører centrale databehandlingsfunktioner ved hjælp af ekstern hukommelse og perifere enheder, herunder mikrokode og anden low-level-firmware. De leverer desuden sikkerhedsrelaterede funktioner såsom kryptering, autentificering, sikker lagring af nøgler, generering af tilfældige tal, pålidelige udførelsesmiljøer eller andre hardwarebaserede beskyttelsesmekanismer, der har til formål at sikre andre produkter, netværk eller tjenester ud over selve mikroprocessoren, såsom secure boot chain, virtualisering eller sikre kommunikationsgrænseflader.
14. Mikrocontrollere med sikkerhedsrelaterede funktioner	Produkter med digitale elementer, som er integrerede kredsløb, der udfører centrale databehandlingsfunktioner med intern hukommelse, der gør mikrocontrolleren programmerbar, og oftest også med perifere enheder, herunder mikrokode og anden low-level-firmware. De leverer desuden sikkerhedsrelaterede funktioner såsom kryptering, autentificering, sikker lagring af nøgler, generering af tilfældige tal, pålidelige udførelsesmiljøer eller andre hardwarebaserede beskyttelsesmekanismer, der har til formål at sikre andre produkter, netværk eller tjenester ud over selve mikrocontrolleren, såsom secure boot chain, virtualisering eller sikre kommunikationsgrænseflader.
15. Applikationsspecifikke integrerede kredsløb (ASIC) og programmerbare porte (FPPT) med sikkerhedsrelaterede funktioner	Applikationsspecifikke integrerede kredsløb (ASIC) med sikkerhedsrelaterede funktioner er produkter med digitale elementer, som er integrerede kredsløb, der er helt eller delvist skræddersyede til at udføre en bestemt funktion eller implementere en specifik applikation, herunder mikrokode og anden low-level-firmware. De leverer desuden sikkerhedsrelaterede funktioner såsom kryptering, autentificering, sikker lagring af nøgler, generering af tilfældige tal, pålidelige udførelsesmiljøer eller andre hardwarebaserede beskyttelsesmekanismer, der har til formål at sikre andre produkter, netværk eller tjenester ud over selve ASIC'en, såsom secure boot chain, virtualisering eller sikre kommunikationsgrænseflader.
	Programmerbare porte (FPGA) med sikkerhedsrelaterede funktioner er produkter med digitale elementer, som er integrerede kredsløb, der er karakteriseret ved en matrix af konfigurerbare logiske blokke, der kan omprogrammeres efter fremstillingen med henblik på at udføre en bestemt funktion eller implementere en specifik applikation, herunder mikrokode og anden low-level-firmware. De leverer desuden sikkerhedsrelaterede funktioner såsom kryptering, autentificering, sikker lagring af nøgler, generering af tilfældige tal, pålidelige udførelsesmiljøer eller andre hardwarebaserede beskyttelsesmekanismer, der har til formål at sikre andre produkter, netværk eller tjenester ud over selve FPGA'en, såsom secure boot chain, virtualisering eller sikre kommunikationsgrænseflader.
16. Virtuelle assistenter til generelle formål i intelligente bygninger	Produkter med digitale elementer, der kommunikerer på det offentlige internet, enten direkte eller via andet udstyr, og behandler input, opgaver eller spørgsmål afgivet i naturligt sprog, f.eks. i form af tale eller skriftligt input, og som på grundlag heraf giver adgang til andre tjenester eller styrer forbundne enheders funktioner i boliger. Denne kategori omfatter, men er ikke begrænset til, intelligente højttalere med en integreret virtuel assistent og enkeltstående virtuelle assistenter, der svarer til denne beskrivelse.

Produktkategori	Teknisk beskrivelse
17. Produkter til intelligente bygninger med sikkerhedsfunktioner, herunder intelligente dørlåse, sikkerhedskameraer, systemer til overvågning af spædbørn og alarmsystemer	Produkter med digitale elementer, der beskytter forbrugernes fysiske sikkerhed i boliger, og som kan fjernstyres fra andre systemer, samt hardware og software, der styrer sådanne produkter centralt. Denne kategori omfatter, men er ikke begrænset til, intelligente dørlåse, systemer til overvågning af spædbørn, alarmsystemer og sikkerhedskameraer til hjemmebrug.
18. Internetforbundet legetøj, der er omfattet af Europa-Parlamentets og Rådets direktiv 2009/48/EF ([1]), og som har sociale interaktive funktioner (f.eks. at det kan tale eller filme), eller som har lokaliseringsfunktioner	Internetforbundet legetøj med sociale interaktive funktioner er produkter med digitale elementer, der er omfattet af direktiv 2009/48/EF, og som kommunikerer på det offentlige internet, enten direkte eller via andet udstyr, og som har indlejrede teknologier, der muliggør indgående og udgående kommunikation, såsom tastatur, mikrofon, højttaler eller kamera.
	Internetforbundet legetøj med lokaliseringsfunktioner er produkter med digitale elementer, der er omfattet af direktiv 2009/48/EF, og som kommunikerer på det offentlige internet, enten direkte eller via andet udstyr, og som har teknologier, der kan fastslå eller udlede legetøjets eller brugerens geografiske placering. Hvis legetøjet kun detekterer brugerens eller andet legetøjs nærhed ved hjælp af sensorteknologier, skal legetøjet ikke anses for at have lokaliseringsfunktioner.
19. Personlige wearable-produkter, der skal bæres af eller anbringes på et menneskelegeme, og som har et sundhedsovervågningsformål (såsom sporing), og som forordning (EU) 2017/745 ([2]) eller (EU) 2017/746 ([3]) ikke finder anvendelse på, eller personlige wearable-produkter, der skal anvendes af og til børn.	Personlige wearable-produkter, der skal bæres af eller anbringes på et menneskelegeme, og som har et sundhedsovervågningsformål, er produkter med digitale elementer, der bæres direkte på kroppen eller via beklædning eller tilbehør, og som regelmæssigt eller kontinuerligt kan indsamle og yderligere behandle data, herunder kropsparametre, der er relevante for brugerens sundhed, undtagen produkter, der er omfattet af anvendelsesområdet for forordning (EU) 2017/745 eller forordning (EU) 2017/746. Denne kategori omfatter, men er ikke begrænset til, fitnesstrackere, smartwatches, intelligente smykker, intelligent beklædning og sportsbeklædning, der svarer til denne beskrivelse.
	Personlige wearable-produkter, der skal anvendes af og til børn, er produkter med digitale elementer, som kan bæres eller anbringes på kroppen, direkte eller via beklædning eller tilbehør, af personer under 14 år. Denne kategori omfatter, men er ikke begrænset til, wearable-sikkerhedsprodukter til børn.

([1]) Europa-Parlamentets og Rådets direktiv 2009/48/EF af 18. juni 2009 om sikkerhedskrav til legetøj (EUT L 170 af 30.6.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, om ændring af direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om ophævelse af Rådets direktiv 90/385/EØF og 93/42/EØF (EUT L 117 af 5.5.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og om ophævelse af direktiv 98/79/EF og Kommissionens afgørelse 2010/227/EU (EUT L 117 af 5.5.2017, s. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Klasse II

Produktkategori	Teknisk beskrivelse
1. Hypervisorer og container runtime-systemer, der understøtter virtuel udførelse af operativsystemer og lignende miljøer	Hypervisorer er softwareprodukter med digitale elementer, der abstraherer og/eller allokerer computerressourcer og muliggør udførelse, styring og organisering af virtuelle maskiner, som er logisk adskilte fra hinanden og/eller fra den fysiske hardware. Hypervisorer kan køre direkte på hardware (»bare metal«), oven på et operativsystem eller i en anden virtuel maskine (»nested virtualisation«). I forbindelse med denne produktkategori er en virtuel maskine et softwaredefineret logisk adskilt computermiljø, som omfatter et virtualiseret sæt hardwareressourcer (f.eks. CPU, hukommelse, lagring, netværksgrænseflader), og som typisk har sit eget operativsystem. Denne kategori omfatter, men er ikke begrænset til, type 1-hypervisorer (»bare metal«), type 2-hypervisorer (hostet på et operativsystem) og hybride hypervisorer.
	Container runtime-systemer er softwareprodukter med digitale elementer, der styrer udførelsen af og livscyklussen for containere, der kører på et enkelt værtsoperativsystem som isolerede processer, og som tildeler ressourcer og muliggør styring og organisering af individuelle containere. I forbindelse med denne produktkategori er en container et softwarebaseret udførelsesmiljø, der indkapsler en eller flere softwarekomponenter og deres afhængigheder i en enkelt pakke, hvilket gør det muligt for den at fungere uafhængigt og konsekvent.
2. Firewalls, systemer til opdagelse og forebyggelse af indtrængen	Firewalls er produkter med digitale elementer, der beskytter et forbundet netværk eller system mod uautoriseret adgang ved at overvåge og begrænse datakommunikationstrafikken til og fra dette netværk. Denne kategori omfatter, men er ikke begrænset til, netværksfirewalls og applikationsfirewalls såsom firewalls til webapplikationer eller filtre og anti-spam-gateways.
	Systemer til opdagelse af indtrængen er produkter med digitale elementer, der overvåger trafikken internt i netværksmiljøet for mistænkelig aktivitet og opdager eller identificerer, at en indtrængen er blevet forsøgt, forekommer eller har fundet sted i et forbundet netværk eller system. Denne kategori omfatter, men er ikke begrænset til, netværksbaserede systemer til opdagelse af indtrængen og værtsbaserede systemer til opdagelse af indtrængen.
	Systemer til forebyggelse af indtrængen er produkter med digitale elementer, der består af et system til opdagelse af indtrængen, der aktivt reagerer på en indtrængen i et forbundet netværk eller system. Denne kategori omfatter, men er ikke begrænset til, netværksbaserede systemer til forebyggelse af indtrængen og værtsbaserede systemer til forebyggelse af indtrængen.

Produktkategori	Teknisk beskrivelse
3. Mikroprocessorer, der er sikret mod manipulation	Produkter med digitale elementer, der er mikroprocessorer med sikkerhedsrelaterede funktioner, jf. tabellen »Klasse I«, punkt 13, i dette bilag, herunder indsamling af beviser for, modstand mod eller respons på manipulation, og som desuden er designet til at yde beskyttelse på AVA_VAN-niveau 2 eller 3 som fastsat i de fælles kriterier og den fælles evalueringsmetode.
4. Mikrocontrollere, der er sikret mod manipulation.	Produkter med digitale elementer, der er mikrocontrollere med sikkerhedsrelaterede funktioner, jf. tabellen »Klasse I«, punkt 14, i dette bilag, herunder indsamling af beviser for, modstand mod eller respons på manipulation, og som desuden er designet til at yde beskyttelse på AVA_VAN-niveau 2 eller 3 som fastsat i de fælles kriterier og den fælles evalueringsmetode.

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

BILAG II

KRITISKE PRODUKTER MED DIGITALE ELEMENTER

Produktkategori	Teknisk beskrivelse
1. Hardwareenheder med sikkerhedsbokse	Hardwareprodukter med digitale elementer, der på sikker vis lagrer, behandler eller forvalter følsomme data eller udfører kryptografiske operationer, og som består af flere diskrete komponenter, der udgør en fysisk hardwareramme, der foretager indsamling af beviser for, modstand mod eller respons på manipulation som modforanstaltninger mod fysiske angreb. Denne kategori omfatter, men er ikke begrænset til, fysiske betalingsterminaler, hardwaresikkerhedsmoduler, der genererer og forvalter kryptografiske elementer, og takografer, der svarer til ovenstående beskrivelse.
2. Gateways til intelligente målere inden for intelligente målersystemer som defineret i artikel 2, nr. 23), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944 ([1]) og andre enheder til avancerede sikkerhedsformål, herunder til sikker krypteringsbehandling.	Gateways til intelligente målere er produkter med digitale elementer, der styrer kommunikationen mellem komponenter, som er del af eller er tilsluttet intelligente målersystemer som defineret i artikel 2, nr. 23), i direktiv (EU) 2019/944, og godkendte tredjeparter såsom forsyningsudbydere. Gateways til intelligente målere indsamler, behandler og lagrer målerdata eller personoplysninger, beskytter data- og informationsstrømme ved at understøtte specifikke kryptografiske behov såsom kryptering og dekryptering af data, indeholder firewall-funktioner og giver mulighed for at styre andre enheder. Denne kategori omfatter, men er ikke begrænset til, gateways til intelligente målere i forbindelse med intelligente målersystemer til måling af elektricitet som defineret i artikel 2, nr. 23), i direktiv (EU) 2019/944. Den kan også omfatte gateways til intelligente målere, der anvendes i andre intelligente målersystemer til måling af forbruget af andre energikilder såsom gas eller varme, forudsat at disse gateways svarer til denne beskrivelse.
3. Smartcards eller lignende enheder, herunder sikre elementer.	Sikre elementer er mikrocontrollere eller mikroprocessorer med sikkerhedsrelaterede funktioner, herunder indsamling af beviser for, modstand mod eller respons på manipulation. Typisk anvendes de til lagring, behandling eller forvaltning af kryptografiske operationer eller følsomme data såsom identitetsoplysninger eller betalingsoplysninger. Sikre elementer er udformet til at yde beskyttelse på mindst AVA_VAN-niveau 4 som fastsat i de fælles kriterier eller den fælles evalueringsmetode. De kan være enten enkeltchip eller integreret i systemer på chip (SoC). Sikre elementer kan indeholde et anvendelsesmiljø eller et operativsystem og kan omfatte en eller flere applikationer. Denne kategori omfatter, men er ikke begrænset til, Trusted Platform Modules (TPM) og embedded Universal Integrated Circuit Cards (UICC).
	Smartcards eller lignende enheder er sikre elementer i form af et kort, der er integreret i et bæremateriale, såsom plast eller træ, eller sikre elementer, der er integreret i bæremateriale med andre former. Denne kategori omfatter, men er ikke begrænset til, identitets- og rejsedokumenter, kvalificerede signaturkort, udskiftelige UICC'er, fysiske betalingskort, fysiske adgangskort, digitale takografkort eller armbånd med integrerede sikre betalingselementer.

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ændring af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).