Uradni list
Evropske unije

SL
Serija L

2025/2392

1.12.2025

IZVEDBENA UREDBA KOMISIJE (EU) 2025/2392

z dne 28. novembra 2025

o tehničnem opisu kategorij pomembnih in kritičnih izdelkov z digitalnimi elementi v skladu z Uredbo (EU) 2024/2847 Evropskega parlamenta in Sveta

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) ([1]), in zlasti člena 7(4) Uredbe,

ob upoštevanju naslednjega:

(1) Uredba (EU) 2024/2847 določa pravila o kibernetski varnosti za izdelke z digitalnimi elementi. Priloga III k navedeni uredbi zlasti določa kategorije pomembnih izdelkov z digitalnimi elementi, za katere se, ko so dani na trg, uporabljajo postopki ugotavljanja skladnosti, ki so strožji od tistih, ki se uporabljajo za druge izdelke z digitalnimi elementi. Priloga IV k Uredbi (EU) 2024/2847 določa kategorije kritičnih izdelkov z digitalnimi elementi, za katere bi se od proizvajalcev lahko zahtevalo, da pridobijo evropski certifikat kibernetske varnosti v okviru evropske certifikacijske sheme za kibernetsko varnost v skladu z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta ([2]), ali za katere bi veljalo obvezno ugotavljanje skladnosti, ki ga opravi tretja oseba, ko se navedeni izdelki dajo na trg.

(2) V skladu s členom 7(1) in členom 8(1) Uredbe (EU) 2024/2847 je od osnovne funkcije izdelka z digitalnimi elementi odvisno, ali navedeni izdelek z digitalnimi elementi ustreza tehničnemu opisu kategorije pomembnih ali kritičnih izdelkov z digitalnimi elementi in s tem veljavne postopke ugotavljanja skladnosti.

(3) Proizvajalci pri razvoju izdelka z digitalnimi elementi in za doseganje želenega nabora funkcij v svoje izdelke z digitalnimi elementi običajno vgradijo druge sestavne dele, ki so prav tako izdelki z digitalnimi elementi in lahko ustrezajo tehničnemu opisu kategorije pomembnih ali kritičnih izdelkov. V skladu z Uredbo (EU) 2024/2847 se za izdelek z digitalnimi elementi uporabljajo postopki ugotavljanja skladnosti, ki se uporabljajo za pomembne ali kritične izdelke z digitalnimi elementi, če je navedeni izdelek kot celota pomembni ali kritični izdelek, kot je določeno v prilogah III in IV k navedeni uredbi. Na primer, vključitev vgrajenega brskalnika kot sestavnega dela aplikacije za novice za uporabo v pametnih telefonih sama po sebi ne pomeni, da za aplikacijo za novice velja postopek ugotavljanja skladnosti, ki se uporablja za izdelke z digitalnimi elementi, ki imajo osnovno funkcijo „samostojnih in vgrajenih brskalnikov“. Kljub temu mora proizvajalec v skladu z Uredbo (EU) 2024/2847 zagotoviti, da izdelek z digitalnimi elementi kot celota izpolnjuje bistvene zahteve glede kibernetske varnosti. Zato mora proizvajalec oceniti varnost celotnega proizvoda in po potrebi upoštevati varnost sestavnih delov ali funkcij, ki so vanj vgrajeni. Da bi na primer proizvajalec aplikacije za novice dokazal, da je njegov izdelek z digitalnimi elementi skladen z Uredbo (EU) 2024/2847, mora dokazati, da aplikacija za novice kot celota izpolnjuje veljavne zahteve, pri čemer se po potrebi upošteva varnost vgrajenega brskalnika, ki je vgrajen v njegovo aplikacijo.

([1]) UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.
([2]) Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Dejstvo, da izdelek z digitalnimi elementi poleg funkcij, navedenih v tehničnih opisih iz te uredbe, opravlja druge ali dodatne funkcije, samo po sebi ne pomeni, da izdelek z digitalnimi elementi nima osnovne funkcije kategorije izdelkov iz prilog III in IV k Uredbi (EU) 2024/2847. Na primer, izdelki z digitalnimi elementi, ki imajo osnovno funkcijo „operacijskih sistemov“, pogosto vključujejo programsko opremo, ki opravlja pomožne funkcije, ki niso vključene v tehnični opis te kategorije izdelkov, kot so npr. kalkulatorji ali preprosti grafični urejevalniki. Izdelki z digitalnimi elementi pogosto vključujejo tudi sestavne dele, ki imajo funkcionalnost drugega pomembnega ali kritičnega izdelka z digitalnimi elementi, kot je operacijski sistem, v katerega je vgrajena funkcija brskalnika, ali usmerjevalnik, v katerega je vgrajena funkcija požarnega zidu. Vendar to samo po sebi ne pomeni, da taki izdelki z digitalnimi elementi nimajo osnovne funkcije „operativnih sistemov“ oziroma „usmerjevalnikov, modemov, namenjenih za povezavo z internetom, in stikal“.

(5) Po drugi strani se za izdelek z digitalnimi elementi, ki lahko opravlja funkcije kategorije izdelkov iz prilog III in IV k Uredbi (EU) 2024/2847, vendar se njegova osnovna funkcija razlikuje od funkcije take kategorije izdelkov, ne šteje, da izpolnjuje tehnični opis navedene kategorije izdelkov. Programska oprema za varnostno organiziranje, avtomatizacijo in odzivanje lahko na primer pogosto opravlja funkcije izdelkov z digitalnimi elementi v kategoriji „varnostni sistem za upravljanje informacij in dogodkov“, tj. zbira podatke, jih analizira in jih predstavlja kot uporabne informacije za varnostne namene. Ker pa njena osnovna funkcija ni funkcija varnostnega sistema za upravljanje informacij in dogodkov, se za programsko opremo varnostno organiziranje, avtomatizacijo in odzivanje na splošno ne šteje, da ustreza tehničnemu opisu „varnostnih sistemov za upravljanje informacij in dogodkov“. Podobno pametni telefon običajno vključuje sestavne dele, ki opravljajo funkcije več kategorij izdelkov iz prilog III in IV k Uredbi (EU) 2024/2847, kot sta npr. operacijski sistem ali vgrajeni upravitelj gesel. Ker pa osnovna funkcija pametnega telefona ni funkcija operacijskega sistema ali upravitelja gesel, se na splošno ne šteje, da ustreza tehničnemu opisu takih kategorij izdelkov.

(6) V skladu s členom 13(2) in (3) Uredbe (EU) 2024/2847 morajo proizvajalci izdelkov z digitalnimi elementi izvajati bistvene zahteve glede kibernetske varnosti iz dela I Priloge I k Uredbi (EU) 2024/2847 na način, ki je sorazmeren s tveganji izdelka z digitalnimi elementi na podlagi predvidenega namena in razumno predvidljive uporabe ter pogojev uporabe izdelka z digitalnimi elementi ob upoštevanju trajanja pričakovane uporabe izdelka. V skladu s členom 13(2) in (3) navedene uredbe in ne glede na to, ali se izdelek z digitalnimi elementi šteje za pomembni ali kritični izdelek z digitalnimi elementi, morajo proizvajalci izvesti celovito oceno tveganja za kibernetsko varnost in navesti, kako se izvajajo bistvene zahteve glede kibernetske varnosti na podlagi ocene tveganja, vključno z njihovim testiranjem in zanesljivostjo. Kadar osnovna funkcija njihovega izdelka z digitalnimi elementi ustreza tehničnemu opisu pomembnega ali kritičnega izdelka z digitalnimi elementi, morajo proizvajalci dokazati skladnost s posebnimi postopki ugotavljanja skladnosti, določenimi v členu 32(2), (3), (4) in (5) Uredbe (EU) 2024/2847.

(7) Ta uredba vključuje primere izdelkov z digitalnimi elementi, katerih osnovna funkcija ustreza tehničnemu opisu določenih pomembnih ali kritičnih izdelkov z digitalnimi elementi. Taki primeri so navedeni le za ponazoritev in niso izčrpen seznam.

(8) Da bi proizvajalcem zagotovili pravno varnost, bi bilo treba kategorije izdelkov z digitalnimi elementi, ki so mikroprocesorji, zaščiteni pred nepooblaščenimi posegi, mikrokrmilniki, zaščiteni pred nepooblaščenimi posegi, ter pametne kartice in podobne naprave, vključno z varnimi elementi, razlikovati glede na stopnjo odpornosti proti morebitni možnosti izkoriščanja napak ali pomanjkljivostim, za katero so bile zasnovane. Raven AVA_VAN je obsežno uporabljen in standardiziran način za izražanje take stopnje odpornosti. Ravni AVA_VAN so določene v javno dostopnih standardih v zvezi s skupnimi merili in skupno metodologijo ocenjevanja, ki so v skladu

z obstoječimi certifikacijskimi okviri, splošno sprejetimi na trgu, kot je Izvedbena uredba Komisije (EU) 2024/482 ([3]). Izvedbena uredba (EU) 2024/482 vzpostavlja evropsko certifikacijsko shemo za kibernetsko varnost, ki se lahko uporablja za certificiranje izdelka na posebni ravni zanesljivosti. Izvedbena uredba (EU) 2024/482 se opira na svetovne prakse in predvideva možnost izdaje certifikatov na podlagi starejših različic standardov do konca leta 2027. Zato je v okviru Uredbe (EU) 2024/2847 primerno dovoliti, da se ravni AVA_VAN izrazijo s sklicevanjem na najnovejšo ali starejše različice navedenih standardov.

(9) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega v skladu s členom 62(1) Uredbe (EU) 2024/2847 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „skupna merila“ pomeni skupna merila za ocenjevanje varnosti informacijske tehnologije, kot so opredeljena v členu 2(1) Izvedbene uredbe (EU) 2024/482 ali kot so določena v standardih iz člena 3(2), točki (a) in (b), navedene izvedbene uredbe;

(2) „skupna metodologija ocenjevanja“ pomeni skupno metodologijo za ocenjevanje varnosti informacijske tehnologije, kot je opredeljena v členu 2(2) Izvedbene uredbe (EU) 2024/482 ali kot je določena v standardih iz člena 3(2), točki (c) in (d), navedene izvedbene uredbe.

Člen 2

1. Tehnični opis kategorij izdelkov z digitalnimi elementi iz razredov I in II iz Priloge III k Uredbi (EU) 2024/2847 je določen v Prilogi I k tej uredbi.

2. Tehnični opis kategorij izdelkov z digitalnimi elementi iz Priloge IV k Uredbi (EU) 2024/2847 je določen v Prilogi II k tej uredbi.

Člen 3

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 28. novembra 2025

Za Komisijo
predsednica
Ursula VON DER LEYEN

([3]) Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 o določitvi pravil za uporabo Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta v zvezi s sprejetjem evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

PRILOGA I

POMEMBNI IZDELKI Z DIGITALNIMI ELEMENTI

Razred I

Kategorija izdelkov	Tehnični opis
1. Programska oprema za sisteme za upravljanje identitete ter programska in strojna oprema za upravljanje privilegiranih dostopov, vključno z bralniki za avtentikacijo uporabnika in nadzor dostopa, vključno z biometričnimi bralniki.	Sistemi za upravljanje identitete so izdelki z digitalnimi elementi, ki zagotavljajo mehanizme za avtentikacijo ali odobritev in lahko zagotavljajo tudi mehanizme za upravljanje življenjskega cikla identifikacijskih poverilnic fizičnih oseb, pravnih oseb, naprav ali sistemov, kot so registracija identitete, njeno dajanje na voljo in vzdrževanje ter izbris. Ti sistemi vključujejo sisteme za upravljanje dostopa, ki nadzorujejo dostop fizičnih oseb, pravnih oseb, naprav ali sistemov do digitalnih virov ali fizičnih lokacij. Programska oprema za upravljanje privilegiranega dostopa je sistem za upravljanje dostopa, ki nadzoruje in spremlja pravice dostopa do sistemov IT ali OT in občutljivih informacij v organizaciji, vključno s sistemi, ki uveljavljajo diferencirane politike nadzora dostopa za privilegirane uporabnike. Ta kategorija med drugim vključuje bralnike za avtentikacijo in nadzor dostopa, biometrične bralnike, programsko opremo za enkratno prijavo, zvezno programsko opremo za upravljanje identitete, programsko opremo za enkratno geslo, naprave za avtentikacijo strojne opreme, kot so generatorji številke za avtentikacijo transakcije (TAN), programska oprema za avtentikacijo in večfaktorska programska oprema za avtentikacijo.
2. Samostojni in vgrajeni brskalniki	Programski izdelki z digitalnimi elementi, ki končnim uporabnikom omogočajo dostop do spletnih vsebin in storitev, ki gostujejo na strežnikih, povezanih z omrežji, kot je internet, ter njihovo prikazovanje in interakcijo z njimi. Običajno vključujejo brskalnik za tolmačenje in prikazovanje vsebin, zapisanih v označevalnem jeziku (npr. HTML), podporo za spletne protokole (npr. HTTP, HTTPS), zmožnost izvrševanja skriptov in upravljanja vnosov uporabnikov ter shranjevanje začasnih ali stalnih podatkov s spletišč (piškotki). Ta kategorija med drugim vključuje samostojne aplikacije, ki izpolnjujejo funkcije brskalnikov, vgrajenih brskalnikov, namenjenih vgraditvi v drug sistem ali aplikacijo, ter brskalnikov z integracijo agentov umetne inteligence.
3. Upravitelji gesel	Izdelki z digitalnimi elementi, ki shranjujejo gesla lokalno na napravi ali na oddaljenem strežniku, vključno z dejavnostmi, kot so ustvarjanje in souporaba gesel ter povezovanje z lokalnimi aplikacijami ali aplikacijami tretjih oseb za uporabo gesel. Ta kategorija med drugim vključuje lokalne upravitelje gesel, upravitelje gesel, ki so na voljo kot razširitve brskalnikov, upravitelje gesel v podjetjih in upravitelje gesel, ki temeljijo na strojni opremi.

Kategorija izdelkov	Tehnični opis
4. Programska oprema, ki išče, odstranjuje ali daje v karanteno zlonamerno programsko opremo.	Programski izdelki z digitalnimi elementi, ki se običajno imenujejo protivirusna ali protizlonamerna programska oprema, ki zaznajo ali iščejo zlonamerno programsko opremo ali kodo na napravah ali tako programsko opremo ali kodo odstranijo ali dajo v karanteno, da se ohranijo celovitost, zaupnost ali razpoložljivost takih naprav. V okviru te kategorije izdelkov zlonamerna programska oprema pomeni programsko opremo, ki vsebuje zlonamerne lastnosti ali zmogljivosti, ki lahko neposredno ali posredno škodujejo uporabniku in/ali računalniškemu sistemu, kot so virusi, črvi, izsiljevalsko programje, vohunska programska oprema in trojanski konji. Ta kategorija med drugim vključuje programsko opremo, ki zaznava ali išče zlonamerno programsko opremo v realnem času ali ročno, zaznavanje korenskega kompleta in reševalne diske z osnovno funkcijo iskanja, odstranjevanja ali karantene zlonamerne programske opreme.
5. Izdelki z digitalnimi elementi s funkcijo navideznega zasebnega omrežja (VPN)	Izdelki z digitalnimi elementi, ki vzpostavijo šifriran logični predor, ki je zgrajen iz sistemskih virov fizičnega ali navideznega omrežja. Ta kategorija med drugim vključuje stranke navideznega zasebnega omrežja, strežnike navideznega zasebnega omrežja in vstopne točke navideznega zasebnega omrežja.
6. Sistemi za upravljanje omrežja	Izdelki z digitalnimi elementi, ki upravljajo povezane omrežne elemente, kot so strežniki, usmerjevalniki, stikala, delovne postaje, tiskalniki ali mobilne naprave, tako da jih spremljajo in nadzorujejo njihovo omrežno delovanje ter konfiguracijo. Ta kategorija med drugim vključuje sisteme upravljanja od konca do konca in namenske sisteme za upravljanje konfiguracij, kot so krmilniki za programsko določeno omrežje.
7. Varnostni sistemi za upravljanje informacij in dogodkov (SIEM)	Izdelki z digitalnimi elementi, ki zbirajo podatke iz več virov, analizirajo in povezujejo navedene podatke ter jih predstavljajo kot uporabne informacije za namene, povezane z varnostjo, kot so odkrivanje groženj in incidentov, forenzična analiza ali skladnost.
8. Upravitelji zagona	Programski izdelki z digitalnimi elementi, ki upravljajo proces začetnega zagona sistema po vklopu/ponovnem zagonu sistema z zagonom strojne opreme, nalaganjem ali prenosom nadzora v okolje operacijskega sistema ali vire sistema in izbiro možnosti zagona. Ta kategorija med drugim vključuje strojno programsko opremo UEFI, enostopenjske in večstopenjske zagonske nalagalnike.
9. Infrastruktura javnih ključev in programska oprema za izdajanje digitalnih certifikatov	Izdelki z digitalnimi elementi, ki se uporabljajo kot del infrastrukture javnih ključev (PKI), ki upravljajo potrjevanje, ustvarjanje, izdajanje, distribucijo, objavo stanja, podaljšanje ali preklic digitalnih potrdil ali ustvarjanje, shranjevanje, deponiranje, izmenjavo, uničenje ali rotacijo kriptografskih ključev, povezanih s takimi digitalnimi potrdili. Ta kategorija med drugim vključuje sisteme upravljanja ključev, sisteme za upravljanje digitalnih potrdil, odzivnike spletnega protokola za status potrdila in rešitve PKI „vse v enem“.

Kategorija izdelkov	Tehnični opis
10. Fizični in navidezni omrežni vmesniki	Fizični omrežni vmesniki so izdelki z digitalnimi elementi, ki napravo neposredno povezujejo z omrežjem prek vmesnika za aplikacijsko programiranje (API), ki ga zagotavljajo pogoni vmesnika in ki običajno delujejo na plasti podatkovne povezave ter vključujejo adapterje strojne opreme za nosilce prenosa z ustrezno strojno programsko opremo, ki običajno delujejo na fizični plasti in plasti podatkovne povezave. Navidezni omrežni vmesniki so izdelki z digitalnimi elementi, ki neposredno ali posredno povezujejo napravo z omrežjem prek API, ki posnema vmesnike pogonov fizičnih omrežnih vmesnikov, ki običajno delujejo na plasti podatkovne povezave. Ta kategorija med drugim vključuje žične in brezžične omrežne vmesniške kartice, krmilnike in adapterje, kot so Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee ali Fieldbus, ter povsem navidezne samostojne izdelke, kot so vmesniške kartice navideznega omrežja, vmesniki omrežja vsebnikov in vmesniki VPN.
11. Operacijski sistemi	Programski izdelki z digitalnimi elementi, ki zagotavljajo abstraktni vmesnik osnovne strojne opreme in nadzorujejo izvajanje programske opreme ter lahko zagotavljajo storitve, kot so upravljanje in konfiguracija računalniških virov, časovno načrtovanje, nadzor vhodnih in izhodnih podatkov, upravljanje podatkov in zagotavljanje vmesnika, prek katerega aplikacije komunicirajo s sistemskimi viri in perifernimi napravami. Ta kategorija med drugim vključuje operacijske sisteme za delo v realnem času, operacijske sisteme za splošne namene in operacijske sisteme za posebne namene.
12. Usmerjevalniki, modemi, namenjeni povezovanju z internetom, in stikala	Usmerjevalniki so izdelki z digitalnimi elementi, ki vzpostavljajo in nadzorujejo pretok podatkov med različnimi omrežji z izbiro poti z uporabo mehanizmov in algoritmov usmerjevalnih protokolov , ki običajno delujejo na omrežni plasti. Ta kategorija med drugim vključuje žične in brezžične usmerjevalnike, navidezne usmerjevalnike in usmerjevalnike z modemi ali brez njih.
	Modemi, namenjeni za povezavo z internetom, so izdelki strojne opreme z digitalnimi elementi, ki uporabljajo tehnike digitalne modulacije in demodulacije za pretvorbo analognih signalov iz digitalnih signalov in v digitalne signale za komunikacijo na podlagi IP. Ta kategorija med drugim vključuje optične modeme, modeme digitalnega naročniškega voda (DSL), kabelske modeme (DOCSIS), satelitske in celične modeme.
	Stikala so izdelki z digitalnimi elementi, ki zagotavljajo povezljivost med omrežnimi napravami prek mehanizmov paketnega posredovanja in imajo raven upravljanja, ki se običajno izvaja na plasti podatkovne povezave ali omrežni plasti. Ta kategorija med drugim vključuje upravljana stikala, pametna stikala, večplastna stikala, navidezna varnostna stikala, programljiva stikala za programsko določena omrežja, in mostove, kot so brezžične dostopovne točke.

Kategorija izdelkov	Tehnični opis
13. Mikroprocesorji z varnostnimi funkcijami	Izdelki z digitalnimi elementi, ki so integrirana vezja, ki izvajajo osrednje funkcije obdelave, ki temeljijo na zunanjem pomnilniku in perifernih napravah, vključno z mikrokodo in drugo strojno programsko opremo nižje ravni. Poleg tega zagotavljajo funkcije, povezane z varnostjo, kot so šifriranje, avtentikacija, varno shranjevanje ključev, naključno ustvarjanje številk, zaupanja vredno okolje izvrševanja ukazov ali druge zaščitne mehanizme na podlagi strojne opreme, katerih cilj je zavarovati druge izdelke, omrežja ali storitve zunaj samega mikroprocesorja, kot so varna zagonska veriga, virtualizacija ali varni komunikacijski vmesniki.
14. Mikrokrmilniki z varnostnimi funkcijami	Izdelki z digitalnimi elementi, ki so integrirana vezja, ki izvajajo osrednje funkcije obdelave s pomnilnikom, kar mikrokrmilniku omogoča programljivost, običajno pa tudi druge periferne naprave, vključno z mikrokodo in drugo strojno programsko opremo nižje ravni. Poleg tega zagotavljajo funkcije, povezane z varnostjo, kot so šifriranje, avtentikacija, varno shranjevanje ključev, naključno ustvarjanje številk, zaupanja vredno okolje izvrševanja ukazov ali druge zaščitne mehanizme na podlagi strojne opreme, katerih cilj je zavarovati druge izdelke, omrežja ali storitve zunaj samega mikroprocesorja, kot so varna zagonska veriga, virtualizacija ali varni komunikacijski vmesniki.
15. Integrirana vezja za določen namen (ASIC) in programljive matrike logičnih vrat (FPGA) z varnostnimi funkcijami	Integrirana vezja za posamezne aplikacije (ASIC) z varnostnimi funkcijami so izdelki z digitalnimi elementi, ki so integrirana vezja, v celoti ali delno prilagojena za opravljanje specifične funkcije ali izvajanje specifične aplikacije, vključno z mikrokodo in drugo strojno programsko opremo nižje ravni. Poleg tega zagotavljajo funkcije, povezane z varnostjo, kot so šifriranje, avtentikacija, varno shranjevanje ključev, naključno ustvarjanje številk, zaupanja vredno okolje izvrševanja ukazov ali druge zaščitne mehanizme na podlagi strojne opreme, katerih cilj je zavarovati druge izdelke, omrežja ali storitve zunaj samega mikroprocesorja, kot so varna zagonska veriga, virtualizacija ali varni komunikacijski vmesniki.
	Programljiva matrika logičnih vrat (FPGA) z varnostnimi funkcijami so izdelki z digitalnimi elementi, ki so integrirana vezja, za katera je značilna matrika logičnih blokov, ki jih je mogoče konfigurirati in ki so zasnovani za programljivost po proizvodnji za opravljanje specifične funkcije ali izvajanje specifične aplikacije, vključno z mikrokodo in drugo strojno programsko opremo nižje ravni. Poleg tega zagotavljajo funkcije, povezane z varnostjo, kot so šifriranje, avtentikacija, varno shranjevanje ključev, naključno ustvarjanje številk, zaupanja vredno okolje izvrševanja ukazov ali druge zaščitne mehanizme na podlagi strojne opreme, katerih cilj je zavarovati druge izdelke, omrežja ali storitve zunaj samega mikroprocesorja, kot so varna zagonska veriga, virtualizacija ali varni komunikacijski vmesniki.
16. Splošni navidezni pomočniki za pametni dom	Izdelki z digitalnimi elementi, ki komunicirajo prek javnega interneta, bodisi neposredno bodisi prek druge opreme, in ki obdelujejo zahteve, naloge ali vprašanja na podlagi naravnega jezika, na primer z zvočnim ali pisnim vnosom, ter ki na podlagi navedenih zahtev, nalog ali vprašanj zagotavljajo dostop do drugih storitev ali nadzorujejo funkcije povezanih naprav v stanovanjskih okoljih. Ta kategorija med drugim vključuje pametne zvočnike z vgrajenim navideznim pomočnikom in samostojne navidezne pomočnike, ki ustrezajo temu opisu.

Kategorija izdelkov	Tehnični opis
17. Izdelki za pametni dom z varnostnimi funkcijami, vključno s pametnimi ključavnicami, varnostnimi kamerami, sistemi za spremljanje dojenčkov in alarmnimi sistemi	Izdelki z digitalnimi elementi, ki ščitijo fizično varnost potrošnikov v stanovanjskem okolju in ki jih je mogoče krmiliti ali upravljati na daljavo iz drugih sistemov, ter strojna in programska oprema, ki centralno nadzorujeta take izdelke. Ta kategorija med drugim vključuje pametne naprave za zaklepanje vrat, sisteme za spremljanje dojenčkov, alarmne sisteme in domače varnostne kamere.
18. Z internetom povezane igrače, zajete v Direktivi 2009/48/ES Evropskega parlamenta in Sveta ([1]), ki imajo funkcije socialne interakcije (npr. govorjenje ali snemanje) ali imajo funkcije za sledenje lokaciji.	Z internetom povezane igrače, ki imajo družabne interaktivne funkcije, so izdelki z digitalnimi elementi, ki jih zajema Direktiva 2009/48/ES, ki komunicirajo prek javnega interneta, bodisi neposredno bodisi prek katere koli druge opreme, in ki imajo vgrajene tehnologije, ki omogočajo vhodno in izhodno komunikacijo, kot so tipkovnica, mikrofon, zvočnik ali kamera.
	Z internetom povezane igrače, ki imajo funkcije sledenja lokaciji, so izdelki z digitalnimi elementi, ki jih zajema Direktiva 2009/48/ES, in ki komunicirajo prek javnega interneta, bodisi neposredno bodisi prek katere koli druge opreme, ter ki imajo tehnologije, ki omogočajo sledenje geografski lokaciji igrače ali uporabnika ali sklepanje o njej. Če igrača zgolj zazna bližino uporabnika ali drugih igrač z uporabo tehnologij zaznavanja, se za igračo ne šteje, da ima funkcije sledenja lokaciji.
19. Osebni nosljivi izdelki, ki so namenjeni nošenju ali namestitvi na človeško telo za namene spremljanja zdravja (kot je sledenje) in za katere se ne uporablja Uredba (EU) 2017/745 ([2]) ali Uredba (EU) 2017/746 Evropskega parlamenta in Sveta ([3]), ali osebni nosljivi izdelki, namenjeni uporabi pri otrocih in za otroke	Osebni nosljivi izdelki, ki se nosijo ali se namestijo na človeško telo z namenom spremljanja zdravja, so izdelki z digitalnimi elementi, ki se nosijo na telesu neposredno ali na oblačilih ali dodatkih, in ki lahko redno ali stalno zaznavajo in nadalje obdelujejo informacije, vključno z merjenjem telesnih vrednosti, ki so pomembne za zdravje uporabnika, razen izdelkov, ki spadajo na področje uporabe Uredbe (EU) 2017/745 ali Uredbe (EU) 2017/746. Ta kategorija med drugim vključuje sledilnike dejavnosti, pametne ure, pametni nakit, pametna oblačila in športna oblačila, ki ustrezajo temu opisu.
	Osebni nosljivi izdelki, namenjeni uporabi s strani otrok in za otroke, so izdelki z digitalnimi elementi, ki jih je mogoče nositi ali namestiti na telo, neposredno ali na oblačila ali dodatke, posameznikov, mlajših od 14 let. Ta kategorija med drugim vključuje nosljive varnostne naprave za otroke.

([1]) Direktiva 2009/48/ES Evropskega parlamenta in Sveta z dne 18. junija 2009 o varnosti igrač (UL L 170, 30.6.2009, str. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o *in vitro* diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Razred II

Kategorija izdelkov	Tehnični opis
1. Hipervizorji in izvajalni sistemi vsebnika, ki podpirajo virtualizirano delovanje operacijskih sistemov in podobnih okolij	Hipervizorji so izdelki programske opreme z digitalnimi elementi, ki abstrahirajo in/ali dodeljujejo računalniške vire ter omogočajo izvrševanje ukazov, upravljanje in organiziranje navideznih strojev, ki so logično ločeni med seboj in/ali od fizične strojne opreme. Hipervizorji lahko delujejo neposredno na podlagi strojne opreme (gola kovina), poleg operacijskega sistema ali v drugem navideznem stroju (ugnezdena virtualizacija). V okviru te kategorije izdelkov je navidezni stroj logična ločitev računalniškega okolja, ki je opredeljena s programsko opremo, ki vključuje virtualiziran sklop virov strojne opreme (npr. centralno procesno enoto, pomnilnik, shranjevanje, omrežne vmesnike) ter običajno gosti lasten operacijski sistem. Ta kategorija med drugim vključuje hipervizorje tipa 1 (gola kovina), hipervizorje tipa 2 (ki gostujejo na operacijskem sistemu) in hibridne hipervizorje.
	Izvajalni sistemi vsebnika so programski izdelki z digitalnimi elementi, ki upravljajo izvrševanje ukazov in življenjski cikel vsebnikov, ki se izvajajo na enem samem gostiteljskem operacijskem sistemu, kot izolirana postopka, pri čemer se dodeljujejo viri ter se omogoča upravljanje in organiziranje posameznih vsebnikov. V okviru te kategorije izdelkov je vsebnik okolje za izvrševanje ukazov na podlagi programske opreme, ki vključuje eno ali več sestavnih delov programske opreme in njihovih odvisnosti v enem samem paketu, kar omogoča neodvisno in dosledno delovanje.
2. Požarni zidovi, sistemi za zaznavanje in preprečevanje vdorov	Požarni zidovi so izdelki z digitalnimi elementi, ki povezano omrežje ali sistem ščitijo pred nepooblaščenim dostopom s spremljanjem in omejevanjem prenosa podatkov v to omrežje in iz njega. Ta kategorija med drugim vključuje omrežne požarne zidove in požarne zidove za aplikacije, kot so požarni zidovi za spletne aplikacije ali filtri in vstopne točke proti neželeni elektronski pošti.
	Sistemi za zaznavanje vdorov so izdelki z digitalnimi elementi, ki spremljajo promet po vstopu v omrežno okolje zaradi sumljive dejavnosti in zaznajo ali ugotovijo, da je prišlo do poskusa vdora v povezano omrežje ali sistem, da vdor poteka ali se je zgodil v povezanem omrežju ali sistemu. Ta kategorija med drugim vključuje omrežne sisteme za zaznavanje vdorov in gostiteljske sisteme za zaznavanje vdorov.
	Sistemi za preprečevanje vdorov so izdelki z digitalnimi elementi, sestavljeni iz sistema za zaznavanje vdorov, ki se dejavno odziva na vdor v povezano omrežje ali sistem. Ta kategorija med drugim vključuje omrežne sisteme za preprečevanje vdorov in gostiteljske sisteme za preprečevanje vdorov.

Kategorija izdelkov	Tehnični opis
3. Mikroprocesorji, zavarovani pred nepooblaščenimi posegi	Izdelki z digitalnimi elementi, ki so mikroprocesorji z varnostnimi funkcijami iz preglednice Razred I, točka 13, te priloge, vključno z dokazi o nepooblaščenih posegih, odpornostjo ali odzivom, in ki so poleg tega zasnovani tako, da zagotavljajo zaščito ravni 2 ali 3 AVA_VAN, kot je določeno v skupnih merilih in skupni metodologiji ocenjevanja.
4. Mikrokrmilniki, zavarovani pred nepooblaščenimi posegi	Izdelki z digitalnimi elementi, ki so mikrokrmilniki z varnostnimi funkcijami iz preglednice Razred I, točka 14, te priloge, vključno z dokazi o nepooblaščenih posegih, odpornostjo ali odzivom na nepooblaščene posege, in ki so poleg tega zasnovani tako, da zagotavljajo zaščito ravni 2 ali 3 AVA_VAN, kot je določeno v skupnih merilih in skupni metodologiji ocenjevanja.

PRILOGA II

KRITIČNI IZDELKI Z DIGITALNIMI ELEMENTI

Kategorija izdelkov	Tehnični opis
1. Naprave strojne opreme z varnostnimi napravami	Izdelki strojne opreme z digitalnimi elementi, ki varno shranjujejo, obdelujejo ali upravljajo občutljive podatke ali izvajajo kriptografske operacije in so sestavljeni iz več diskretnih sestavnih delov ter vključujejo fizični ovoj strojne opreme, ki zagotavlja dokaze o nepooblaščenem posegu, odpornost ali odziv na nepooblaščeni poseg kot protiukrepe proti fizičnim napadom. Ta kategorija med drugim vključuje fizične plačilne terminale, varnostne module strojne opreme, ki ustvarjajo in upravljajo kriptografske elemente, ter tahografe, ki ustrezajo zgornjemu opisu.
2. Vstopne točke za napredne števce v sistemih naprednega merjenja, kot so opredeljeni v členu 2(23), Direktive (EU) 2019/944 Evropskega parlamenta in Sveta ([1]), in druge naprave za napredne varnostne namene, tudi za varno obdelavo kriptosredstev.	Vstopne točke za napredne števce so izdelki z digitalnimi elementi, ki nadzorujejo komunikacijo med sestavnimi deli v sistemih naprednega merjenja, kot so opredeljeni v členu 2(23) Direktive (EU) 2019/944, ali povezanimi z njimi, in pooblaščenimi tretjimi osebami, kot so ponudniki komunalnih storitev. Vstopne točke za napredne števce zbirajo, obdelujejo in shranjujejo merilne ali osebne podatke, ščitijo pretok podatkov in informacij s podpiranjem posebnih kriptografskih potreb, kot sta šifriranje in dešifriranje podatkov, vključujejo funkcije požarnega zidu in zagotavljajo sredstva za krmiljenje drugih naprav. Ta kategorija med drugim vključuje vstopne točke za napredne števce, povezane s sistemi naprednega merjenja, ki merijo električno energijo, kot so opredeljeni v členu 2(23) Direktive (EU) 2019/944. Vključuje lahko tudi vstopne točke za napredne števce, ki se uporabljajo v drugih pametnih merilnih sistemih, ki merijo porabo drugih virov energije, kot sta plin ali toplota, če vstopna točka izpolnjuje ta opis.
3. Pametne kartice ali podobne naprave, vključno z varnimi elementi	Varni elementi so mikrokrmilniki ali mikroprocesorji z varnostnimi funkcijami, vključno z dokazi o nepooblaščenih posegih, odpornosti ali odzivu na nepooblaščene posege. Običajno shranjujejo, obdelujejo ali upravljajo kriptografske operacije ali občutljive podatke, kot so identifikacijske ali plačilne poverilnice. Varni elementi so zasnovani tako, da zagotavljajo zaščito vsaj na ravni AVA_VAN.4, kot je določeno v skupnih merilih ali skupni metodologiji ocenjevanja. Lahko so diskretni silicij ali vgrajeni v sisteme na čipu. V varne elemente je lahko vključeno aplikacijsko okolje ali operacijski sistem ter lahko vključujejo eno ali več aplikacij. Ta kategorija med drugim vključuje module zaupanja vredne platforme in vgrajeno univerzalno pametno kartico (UICC).
	Pametne kartice ali podobne naprave so varni elementi, ki so vgrajeni v nosilni material, kot sta plastika ali les, v obliki kartice, ali varnostni elementi, vgrajeni v nosilne materiale v drugih oblikah. Ta kategorija med drugim vključuje osebne in potovalne dokumente, kvalificirane kartice za podpise, zamenljive univerzalne pametne kartice, fizične plačilne kartice, kartice za fizični dostop, digitalne tahografske kartice ali zapestne trakove z vgrajenimi varnostnimi elementi za plačila.

([1]) Direktiva (EU) 2019/944 Evropskega parlamenta in Sveta z dne 5. junija 2019 o skupnih pravilih notranjega trga električne energije in spremembi Direktive 2012/27/EU (UL L 158, 14.6.2019, str. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).