2025/2392

1.12.2025.

PROVEDBENA UREDBA KOMISIJE (EU) 2025/2392

od 28. studenoga 2025.

o tehničkom opisu kategorija važnih i kritičnih proizvoda s digitalnim elementima na temelju Uredbe (EU) 2024/2847 Europskog parlamenta i Vijeća

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti) ([1]), a posebno njezin članak 7. stavak 4.,

budući da:

(1) Uredbom (EU) 2024/2847 utvrđena su pravila o kibernetičkoj sigurnosti proizvoda s digitalnim elementima. Konkretnije, u Prilogu III. toj uredbi utvrđene su kategorije važnih proizvoda s digitalnim elementima koji, kad se stavljaju na tržište, podliježu strožim postupcima ocjenjivanja sukladnosti od onih primjenjivih na druge proizvode s digitalnim elementima. U Prilogu IV. toj uredbi utvrđene su kategorije kritičnih proizvoda s digitalnim elementima za koje bi se pri stavljanju na tržište od proizvođača moglo zahtijevati da ishode europski kibernetičkosigurnosni certifikat u okviru europskog programa kibernetičkosigurnosne certifikacije na temelju Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća ([2]) ili koji bi podlijegali obveznom ocjenjivanju sukladnosti koje provodi treća strana.

(2) U skladu s člankom 7. stavkom 1. i člankom 8. stavkom 1. Uredbe (EU) 2024/2847 to odgovara li proizvod s digitalnim elementima tehničkom opisu kategorije važnih ili kritičnih proizvoda s digitalnim elementima, a stoga i koji su postupci ocjenjivanja sukladnosti primjenjivi, ovisi o osnovnoj funkcionalnosti tog proizvoda.

(3) Kako bi postigli željeni skup funkcionalnosti, proizvođači u svoje proizvode s digitalnim elementima u obično integriraju druge komponente koje su same po sebi također proizvodi s digitalnim elementima i koje mogu odgovarati tehničkom opisu kategorije važnih ili kritičnih proizvoda. U skladu s Uredbom (EU) 2024/2847 proizvod s digitalnim elementima podliježe postupcima ocjenjivanja sukladnosti primjenjivima na važne ili kritične proizvode s digitalnim elementima ako je u cjelini važan ili kritičan proizvod kako je utvrđeno u prilozima III. i IV. toj uredbi. Na primjer, integracija ugrađenog preglednika u aplikaciju za vijesti za pametne telefone sama po sebi ne znači da ta aplikacija podliježe postupku ocjenjivanja sukladnosti primjenjivom na proizvode s digitalnim elementima koji imaju osnovnu funkcionalnost „samostalnih i ugrađenih preglednika”. Ipak, prema Uredbi (EU) 2024/2847 proizvođač mora osigurati da proizvod s digitalnim elementima u cjelini ispunjava bitne zahtjeve u pogledu kibernetičke sigurnosti. To znači da mora ocijeniti sigurnost cijelog proizvoda, pri čemu, prema potrebi, treba uzeti u obzir sigurnost integriranih komponenata ili funkcionalnosti. Na primjer, da bi proizvođač aplikacije za vijesti dokazao da je njegov proizvod s digitalnim elementima sukladan s Uredbom (EU) 2024/2847, on mora dokazati da ta aplikacija u cjelini ispunjava primjenjive zahtjeve, pri čemu, prema potrebi, uzima u obzir sigurnost ugrađenog preglednika koji je u nju integriran.

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

([2]) Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Činjenica da proizvod s digitalnim elementima obavlja druge funkcije koje nisu navedene u tehničkim opisima utvrđenima u ovoj Uredbi ili dodatne funkcije sama po sebi ne znači da taj proizvod nema osnovnu funkcionalnost kategorije proizvoda iz priloga III. i IV. Uredbi (EU) 2024/2847. Na primjer, proizvodi s digitalnim elementima koji imaju osnovnu funkcionalnost „operativnih sustava" često uključuju softver koji obavlja pomoćne funkcije koje nisu uključene u tehnički opis te kategorije proizvoda, npr. kalkulatore ili jednostavne grafičke uređivače. Proizvodi s digitalnim elementima često sadržavaju i komponente koje imaju funkcionalnost drugog važnog ili kritičnog proizvoda s digitalnim elementima. To su npr. operativni sustavi s integriranim preglednikom ili ruteri s integriranim vatrozidom. To, međutim, samo po sebi ne znači da takvi proizvodi s digitalnim elementima nemaju osnovnu funkcionalnost „operativnih sustava" ili „rutera, modema namijenjenih za spajanje na internet i preklopnika".

(5) S druge strane, za proizvod s digitalnim elementima koji može obavljati funkcije kategorije proizvoda iz priloga III. i IV. Uredbi (EU) 2024/2847, ali čija se osnovna funkcionalnost razlikuje od osnovne funkcionalnosti te kategorije proizvoda smatra se da ne odgovara tehničkom opisu te kategorije proizvoda. Na primjer, softver za sigurnosnu orkestraciju, automatizaciju i odgovor (SOAR) često može obavljati funkcije proizvoda s digitalnim elementima iz kategorije „sustavi za upravljanje sigurnosnim informacijama i događajima (SIEM)", odnosno prikupljati podatke, analizirati ih i prikazivati kao upotrebljive informacije za sigurnosne potrebe. Međutim, budući da njegova osnovna funkcionalnost nije ona SIEM-a, za SOAR se općenito smatra da ne odgovara tehničkom opisu „sustava za upravljanje sigurnosnim informacijama i događajima (SIEM)". Slično tome, u pametni telefon obično su integrirane komponente koje obavljaju funkcije više kategorija proizvoda iz priloga III. i IV. Uredbi (EU) 2024/2847, npr. operativni sustav ili integrirani upravitelj lozinki. Međutim, budući da njegova osnovna funkcionalnost nije operativni sustav ili upravitelj lozinki, općenito se smatra da ne odgovara tehničkom opisu tih kategorija proizvoda.

(6) Prema članku 13. stavcima 2. i 3. Uredbe (EU) 2024/2847 proizvođači proizvoda s digitalnim elementima moraju provoditi bitne zahtjeve u pogledu kibernetičke sigurnosti iz dijela I. Priloga I. Uredbi (EU) 2024/2847 na način koji je razmjeran rizicima proizvoda s digitalnim elementima s obzirom na namjenu i razumno predvidljivu upotrebu te uvjete njihove upotrebe, uzimajući u obzir očekivano trajanje upotrebe proizvoda. U skladu s člankom 13. stavcima 2. i 3. te uredbe, i neovisno o tome smatra li se proizvod s digitalnim elementima važnim ili kritičnim proizvodom s digitalnim elementima, proizvođači moraju provesti sveobuhvatnu procjenu kibernetičkosigurnosnog rizika i navesti kako se bitni zahtjevi u pogledu kibernetičke sigurnosti provode na temelju te procjene, što uključuje njihovo ispitivanje i jamstvo. Ako osnovna funkcionalnost njihova proizvoda s digitalnim elementima odgovara tehničkom opisu važnog ili kritičnog proizvoda s digitalnim elementima, proizvođači moraju dokazati sukladnost primjenom odgovarajućih postupaka ocjenjivanja sukladnosti iz članka 32. stavaka 2., 3., 4. i 5. Uredbe (EU) 2024/2847.

(7) Ova Uredba uključuje primjere proizvoda s digitalnim elementima čija osnovna funkcionalnost odgovara tehničkom opisu određenih važnih ili kritičnih proizvoda s digitalnim elementima. Ti su primjeri samo ilustrativni i ne čine potpun popis.

(8) Kako bi proizvođači imali pravnu sigurnost, kategorije proizvoda s digitalnim elementima koji su mikroprocesori otporni na manipuliranje, mikrokontroleri otporni na manipuliranje te pametne kartice i slični uređaji, uključujući sigurne elemente, trebalo bi razlikovati prema stupnju otpornosti na potencijalno iskorištavanje nedostataka ili slabosti za koje su projektirani. Standardiziran i uobičajen način izražavanja tog stupnja otpornosti je razina AVA_VAN. Razine AVA_VAN utvrđene su u javno dostupnim normama za zajedničke kriterije i zajedničku evaluacijsku metodologiju, na kojima se temelje postojeći okviri za certifikaciju koji su općeprihvaćeni na tržištu,

kao što je Provedbena uredba Komisije (EU) 2024/482 ([3]). Tom se uredbom uspostavlja europski program kibernetičkosigurnosne certifikacije kojim se proizvodi mogu certificirati na određenu razinu jamstva i, u skladu s globalnom praksom, mogućnost izdavanja certifikata na temelju starijih verzija normi predviđena je do kraja 2027. Stoga je u kontekstu te uredbe primjereno dopustiti da se razine AVA_VAN izražavaju upućivanjem ili na najnoviju verziju ili na starije verzije tih normi.

(9) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 62. stavkom 1. Uredbe (EU) 2024/2847,

DONIJELA JE OVU UREDBU:

Članak 1.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „zajednički kriteriji” znači zajednički kriteriji za evaluaciju sigurnosti informacijske tehnologije kako su definirani u članku 2. stavku 1. Provedbene uredbe (EU) 2024/482 ili kako su utvrđeni u normama iz članka 3. stavka 2. točaka (a) i (b) te provedbene uredbe;
2. „zajednička evaluacijska metodologija” znači Zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije kako je definirana u članku 2. stavku 2. Provedbene uredbe (EU) 2024/482 ili kako je utvrđena u normama iz članka 3. stavka 2. točaka (c) i (d) te provedbene uredbe.

Članak 2.

1. Tehnički opis kategorija proizvoda s digitalnim elementima I. i II. razreda iz Priloga III. Uredbi (EU) 2024/2847 utvrđuje se u Prilogu I. ovoj Uredbi.

2. Tehnički opis kategorija proizvoda s digitalnim elementima iz Priloga IV. Uredbi (EU) 2024/2847 utvrđuje se u Prilogu II. ovoj Uredbi.

Članak 3.

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 28. studenoga 2025.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

([3]) Provedbena uredba Komisije (EU) 2024/482 od 31. siječnja 2024. o utvrđivanju pravila za primjenu Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća u pogledu donošenja europskog programa kibernetičkosigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) (SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

PRILOG I.

VAŽNI PROIZVODI S DIGITALNIM ELEMENTIMA

I. razred

Kategorija proizvoda	Tehnički opis
1. Sustavi za upravljanje identitetom te softver i hardver za upravljanje povlaštenim pristupom, uključujući čitače za provjeru autentičnosti i kontrolu pristupa, uključujući biometrijske čitače	Sustavi za upravljanje identitetom su proizvodi s digitalnim elementima koji pružaju mehanizme za autentifikaciju ili autorizaciju i koji također mogu pružati mehanizme za upravljanje životnim ciklusom identifikacijskih vjerodajnica fizičkih osoba, pravnih osoba, uređaja ili sustava, kao što su registracija, pribavljanje, održavanje i deregistracija identiteta. Ti sustavi obuhvaćaju sustave za upravljanje pristupom koji kontroliraju pristup fizičkih osoba, pravnih osoba, uređaja ili sustava digitalnim resursima ili fizičkim lokacijama. Softver za upravljanje povlaštenim pristupom sustav je za upravljanje pristupom koji kontrolira i prati prava pristupa IT ili OT sustavima i osjetljivim informacijama unutar organizacije, što uključuje sustave kojima se provode pravila kontrole diferenciranog pristupa za povlaštene korisnike. Kategorija obuhvaća, među ostalim, i čitače za autentifikaciju i kontrolu pristupa, biometrijske čitače, softver za jedinstvenu prijavu, softver za upravljanje federalnim identitetom, softver za jednokratne lozinke, hardverske uređaje za autentifikaciju kao što su generatori brojeva za autentifikaciju transakcije (TAN), softver za autentifikaciju i softver za višefaktorsku autentifikaciju.
2. Samostalni i ugrađeni preglednici	Softverski proizvodi s digitalnim elementima koji krajnjim korisnicima omogućuju pristup, prikazivanje i interakciju s *web*-sadržajima i uslugama na poslužiteljima koji su povezani s mrežama kao što je internet. Obično imaju *engine* za tumačenje i prikazivanje sadržaja na jeziku za označavanje (npr. HTML), podršku za mrežne protokole (npr. HTTP, HTTPS), sposobnost izvršavanja skripti i upravljanja korisničkim unosima te pohranu privremenih ili trajnih podataka s internetskih stranica (kolačići). Kategorija obuhvaća, među ostalim, samostalne aplikacije koje obavljaju funkcije preglednika, ugrađene preglednike namijenjene za integraciju u drugi sustav ili aplikaciju i preglednike s integriranim UI agentima.
3. Upravitelji lozinki	Proizvodi s digitalnim elementima koji pohranjuju lozinke na lokalnom uređaju ili na udaljenom poslužitelju, uključujući aktivnosti kao što su generiranje lozinki, dijeljenje lozinki i integracija s lokalnim aplikacijama ili aplikacijama treće strane za korištenje lozinki. Kategorija obuhvaća, među ostalim, lokalne upravitelje lozinki, upravitelje lozinki u obliku proširenja preglednika, upravitelje lozinki za poduzeća i hardverske upravitelje lozinki.

Kategorija proizvoda	Tehnički opis
4. Softver za traženje, uklanjanje ili izoliranje zlonamjernog softvera	Softverski proizvodi s digitalnim elementima, obično poznati kao antivirusni programi ili programi protiv zlonamjernog softvera, koji otkrivaju, traže, uklanjaju ili stavljaju u karantenu zlonamjerni softver ili kod na uređajima kako bi očuvali integritet, povjerljivost ili dostupnost uređaja. U kontekstu ove kategorije proizvoda zlonamjerni softver znači softver koji ima zlonamjerne značajke ili sposobnosti koje mogu izravno ili neizravno nanijeti štetu korisniku i/ili računalnom sustavu, kao što su virusi, crvi, ucjenjivački softver, špijunski programi i trojanci. Kategorija obuhvaća, među ostalim, softver koji otkriva ili traži zlonamjerni softver u stvarnom vremenu ili ručno, alate za otkrivanje *rootkita* i diskove za spašavanje s osnovnom funkcijom traženja, uklanjanja ili stavljanja zlonamjernog softvera u karantenu.
5. Proizvodi s digitalnim elementima s funkcijom virtualne privatne mreže (VPN)	Proizvodi s digitalnim elementima koji uspostavljaju šifrirani logički tunel sastavljen od resursa sustava fizičke ili virtualne mreže. Kategorija obuhvaća, među ostalim, VPN klijente, poslužitelje i pristupnike.
6. Sustavi za upravljanje mrežom	Proizvodi s digitalnim elementima koji upravljaju povezanim elementima mreže kao što su poslužitelji, ruteri, preklopnici, radne stanice, pisači ili mobilni uređaji tako što ih nadziru i kontroliraju njihov mrežni rad i konfiguraciju. Kategorija obuhvaća, među ostalim, sustave za upravljanje cijelim procesom (*end-to-end*) i namjenske sustave za upravljanje konfiguracijom, kao što su kontroleri za softverski definirano umrežavanje.
7. Sustavi za upravljanje sigurnosnim informacijama i događajima (SIEM)	Proizvodi s digitalnim elementima koji prikupljaju, analiziraju i povezuju podatke iz više izvora te ih prikazuju kao upotrebljive informacije za sigurnosne potrebe kao što su otkrivanje prijetnji i incidenata, forenzička analiza ili postizanje sukladnosti.
8. Upravitelji pokretanja sustava	Softverski proizvodi s digitalnim elementima koji upravljaju procesom početnog pokretanja sustava nakon njegova uključivanja / ponovnog pokretanja tako što inicijaliziraju hardver, učitavaju ili prenose kontrolu na okruženje operativnog sustava ili resurse sustava i odabiru opcije za pokretanje sustava. Kategorija obuhvaća, među ostalim, UEFI ugrađeni softver te jednostupanjske i višestupanjske učitavače za pokretanje sustava (*boot loaders*).
9. Infrastruktura javnih ključeva i softver za izdavanje digitalnih certifikata	Proizvodi s digitalnim elementima koji se upotrebljavaju kao dio infrastrukture javnih ključeva (PKI) i upravljaju validacijom, kreiranjem, izdavanjem, distribucijom, objavom statusa, obnavljanjem ili opozivom digitalnih certifikata ili stvaranjem, pohranom, povjeravanjem, razmjenom, uništavanjem ili rotacijom kriptografskih ključeva povezanih s tim digitalnim certifikatima. Ova kategorija uključuje, ali nije ograničena na sustave za upravljanje ključevima, sustave za upravljanje digitalnim certifikatima, poslužitelje za internetsku provjeru statusa certifikata i sveobuhvatna rješenja za PKI.

Kategorija proizvoda	Tehnički opis
10. Fizička i virtualna mrežna sučelja	Fizička mrežna sučelja su proizvodi s digitalnim elementima koji izravno povezuju neki uređaj s mrežom putem aplikacijskog programskog sučelja (API) koje pružaju upravljački programi sučelja (obično funkcioniraju na sloju podatkovne veze) i koji imaju hardverske adaptere za prijenosne medije s odgovarajućim ugrađenim softverom (obično funkcioniraju na fizičkom sloju i sloju podatkovne veze). Virtualna mrežna sučelja su proizvodi s digitalnim elementima koji izravno ili neizravno povezuju uređaj s mrežom putem API-ja koji emulira sučelje upravljačkih programa fizičkih mrežnih sučelja (obično funkcioniraju na sloju podatkovne veze). Kategorija obuhvaća, među ostalim, kartice, kontrolere i adaptere žičanih i bežičnih mrežnih sučelja, kao što su Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee ili Fieldbus, te potpuno virtualne samostalne proizvode kao što su virtualne mrežne kartice, mrežna sučelja spremnika i VPN sučelja.
11. Operativni sustavi	Softverski proizvodi s digitalnim elementima koji daju apstraktno sučelje temeljnog hardvera i kontroliraju izvršenje softvera te koji mogu pružati usluge kao što su upravljanje računalnim resursima i njihovo konfiguriranje, planiranje, kontrola ulaza i izlaza, upravljanje podacima i pružanje sučelja kojim aplikacije komuniciraju s resursima sustava i perifernim uređajima. Kategorija obuhvaća, među ostalim, operativne sustave u stvarnom vremenu, operativne sustave opće namjene i operativne sustave posebne namjene.
12. Ruteri, modemi namijenjeni za spajanje na internet i preklopnici	Ruteri su proizvodi s digitalnim elementima koji uspostavljaju i kontroliraju protok podataka između različitih mreža tako što odabiru putove ili rute pomoću mehanizama i algoritama protokola usmjeravanja (obično funkcioniraju na mrežnom sloju). Kategorija obuhvaća, među ostalim, žičane i bežične rutere, virtualne rutere i rutere s modemima ili bez njih.
	Modemi za spajanje na internet hardverski su proizvodi s digitalnim elementima koji tehnikama digitalne modulacije i demodulacije pretvaraju analogne signale u digitalne signale i obrnuto za potrebe komunikacije na temelju IP-a. Kategorija obuhvaća, među ostalim, svjetlovodne modeme, modeme digitalne pretplatničke linije (DSL), kabelske modeme (DOCSIS), satelitske modeme i celularne modeme.
	Preklopnici su proizvodi s digitalnim elementima koji omogućuju povezivanje umreženih uređaja mehanizmima za prosljeđivanje paketa i koji imaju upravljačku razinu, obično na sloju podatkovne veze ili mreže. Kategorija obuhvaća, među ostalim, upravljane preklopnike, pametne preklopnike, višeslojne preklopnike, virtualne sigurnosne preklopnike, programirljive preklopnike za softverski definirano umrežavanje i mostove kao što su bežične pristupne točke.

Kategorija proizvoda	Tehnički opis
13. Mikroprocesori s funkcijama povezanima sa sigurnošću	Proizvodi s digitalnim elementima koji su integrirani krugovi koji obavljaju funkcije središnje obrade oslanjajući se na vanjsku memoriju i periferne uređaje, što uključuje mikrokod i drugi ugrađeni softver niske razine. Uz to, obavljaju funkcije povezane sa sigurnošću, kao što su šifriranje, autentifikacija, sigurna pohrana ključeva, generiranje nasumičnih brojeva, pouzdano okruženje za izvršavanje ili drugi hardverski zaštitni mehanizmi, radi zaštite drugih proizvoda, mreža ili usluga izvan samog mikroprocesora, kao što su lanac sigurnog pokretanja sustava, virtualizacija ili sigurna komunikacijska sučelja.
14. Mikrokontroleri s funkcijama povezanima sa sigurnošću	Proizvodi s digitalnim elementima koji su integrirani krugovi s integriranom memorijom koji obavljaju funkcije središnje obrade, što omogućava programiranje mikrokontrolera i obično drugih perifernih uređaja, uključujući mikrokod i drugi ugrađeni softver niske razine. Uz to, obavljaju funkcije povezane sa sigurnošću, kao što su šifriranje, autentifikacija, sigurna pohrana ključeva, generiranje nasumičnih brojeva, pouzdano okruženje za izvršavanje ili drugi hardverski zaštitni mehanizmi, radi zaštite drugih proizvoda, mreža ili usluga izvan samog mikrokontrolera, kao što su lanac sigurnog pokretanja sustava, virtualizacija ili sigurna komunikacijska sučelja.
15. Integrirani krugovi specijalizirane namjene (ASIC) i programirljivi logički sklopovi (FPGA) s funkcijama povezanima sa sigurnošću	Integrirani krugovi specijalizirane namjene (ASIC) s funkcijama povezanima sa sigurnošću su proizvodi s digitalnim elementima koji su integrirani krugovi potpuno ili djelomično projektirani za izvršavanje specifične funkcije ili aplikacije, što uključuje mikrokod i drugi ugrađeni softver niske razine. Uz to, obavljaju funkcije povezane sa sigurnošću, kao što su šifriranje, autentifikacija, sigurna pohrana ključeva, generiranje nasumičnih brojeva, pouzdano okruženje za izvršavanje ili drugi hardverski zaštitni mehanizmi, radi zaštite drugih proizvoda, mreža ili usluga izvan samog ASIC-a, kao što su lanac sigurnog pokretanja sustava, virtualizacija ili sigurna komunikacijska sučelja.
	Programirljivi logički sklopovi (FPGA) s funkcijama povezanima sa sigurnošću su proizvodi s digitalnim elementima koji su integrirani krugovi s matricom konfigurabilnih logičkih blokova projektirani tako da se mogu reprogramirati nakon proizvodnje za obavljanje određene funkcije ili implementaciju određene aplikacije, što uključuje mikrokod i drugi ugrađeni softver niske razine. Uz to, obavljaju funkcije povezane sa sigurnošću, kao što su šifriranje, autentifikacija, sigurna pohrana ključeva, generiranje nasumičnih brojeva, pouzdano okruženje za izvršavanje ili drugi hardverski zaštitni mehanizmi, radi zaštite drugih proizvoda, mreža ili usluga izvan samih FPGA-ova, kao što su lanac sigurnog pokretanja sustava, virtualizacija ili sigurna komunikacijska sučelja.
16. Virtualni asistenti opće namjene za pametne kuće	Proizvodi s digitalnim elementima koji izravno ili posredstvom druge opreme komuniciraju na javnom internetu, obrađuju zahtjeve, zadaće ili pitanja na temelju prirodnojezičnih upita, primjerice u zvučnom ili tekstnom obliku, i na temelju tih zahtjeva, zadaća ili pitanja omogućuju pristup drugim uslugama ili upravljaju funkcijama povezanih uređaja u stambenim okruženjima. Kategorija obuhvaća, među ostalim, pametne zvučnike s integriranim virtualnim asistentom i samostalne virtualne asistente koji odgovaraju prethodnom opisu.

Kategorija proizvoda	Tehnički opis
17. Proizvodi za pametne kuće sa sigurnosnim funkcijama, uključujući pametne brave za vrata, sigurnosne kamere, sustave za nadzor male djece i alarmne sustave	Proizvodi s digitalnim elementima koji služe za fizičku zaštitu potrošača u stambenom okruženju i kojima se može upravljati na daljinu iz drugih sustava te hardver i softver za središnje upravljanje tim proizvodima. Kategorija obuhvaća, među ostalim, pametne uređaje za zaključavanje vrata, sustave za nadzor male djece, alarmne sustave i kućne sigurnosne kamere.
18. Igračke povezane s internetom obuhvaćene Direktivom 2009/48/EZ Europskog parlamenta i Vijeća ([1]) koje imaju društvene interaktivne značajke (npr. govor ili snimanje) ili imaju značajke praćenja lokacije	Igračke povezane s internetom koje imaju društvene interaktivne značajke su proizvodi s digitalnim elementima obuhvaćeni Direktivom 2009/48/EZ koji izravno ili posredstvom druge opreme komuniciraju na javnom internetu i imaju ugrađene uređaje koji omogućuju ulaznu i izlaznu komunikaciju, npr. tipkovnicu, mikrofon, zvučnik ili kameru.
	Igračke povezane s internetom koje imaju značajke praćenja lokacije su proizvodi s digitalnim elementima obuhvaćeni Direktivom 2009/48/EZ koji izravno ili posredstvom druge opreme komuniciraju na javnom internetu i imaju tehnologije koje omogućuju praćenje ili izvođenje zemljopisne lokacije igračke ili njezina korisnika. Ako igračka pomoću senzorskih tehnologija samo otkriva jesu li korisnik ili druge igračke u njezinoj blizini, smatra se da nema značajke praćenja lokacije.
19. Osobni nosivi proizvodi koje treba nositi ili staviti na ljudsko tijelo i koji imaju svrhu praćenja zdravlja (kao što je praćenje) i na koje se ne primjenjuju Uredba (EU) 2017/745 ([2]) ili Uredba (EU) 2017/746 Europskog parlamenta i Vijeća ([3]) ili osobni nosivi proizvodi koji su namijenjeni za upotrebu od strane djece ili za djecu	Osobni nosivi proizvodi koje treba nositi ili staviti na ljudsko tijelo i koji imaju svrhu praćenja zdravlja su proizvodi s digitalnim elementima koji se izravno ili putem odjeće ili dodataka nose na tijelu i koji redovito ili kontinuirano mogu otkrivati i dodatno obrađivati informacije relevantne za zdravlje korisnika, uključujući tjelesnu metriku, osim proizvoda obuhvaćenih područjem primjene Uredbe (EU) 2017/745 ili Uredbe (EU) 2017/746. Kategorija obuhvaća, među ostalim, uređaje za praćenje kondicije, pametne satove, pametni nakit, pametnu odjeću i sportsku odjeću koja odgovara prethodnom opisu.
	Osobni nosivi proizvodi koji su namijenjeni za upotrebu od strane djece ili za djecu su proizvodi s digitalnim elementima koje izravno ili pomoću odjeće ili dodataka mogu nositi ili staviti na tijelo osobe mlađe od 14 godina. Kategorija obuhvaća, među ostalim, sigurnosne dječje nosive uređaje.

([1]) Direktiva 2009/48/EZ Europskog parlamenta i Vijeća od 18. lipnja 2009. o sigurnosti igračaka (SL L 170, 30.6.2009., str. 1., ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (SL L 117, 5.5.2017., str. 1., ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o *in vitro* dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (SL L 117, 5.5.2017., str. 176., ELI: http://data.europa.eu/eli/reg/2017/746/oj).

II. razred

Kategorija proizvoda	Tehnički opis
1. Hipervizori i sustavi za izolirano izvršavanje koji omogućuju virtualizirano izvršavanje operativnih sustava i slična okruženja	Hipervizori su softverski proizvodi s digitalnim elementima koji apstrahiraju i/ili dodjeljuju računalne resurse i omogućuju izvršavanje, upravljanje i orkestraciju virtualnih strojeva koji su logički odvojeni jedni od drugih i/ili od fizičkog hardvera. Hipervizori mogu raditi izravno na hardveru (*bare metal*), kao aplikacije iznad operativnog sustava ili unutar drugog virtualnog stroja (ugniježđena virtualizacija). U kontekstu te kategorije proizvoda virtualni stroj je softverski definirana logička separacija računalnog okruženja, koja uključuje virtualizirani skup hardverskih resursa (npr. procesor, memorija, pohrana, mrežna sučelja) i obično ima zasebni operativni sustav. Kategorija obuhvaća, među ostalim, hipervizore tipa 1 (*bare metal*), hipervizore tipa 2 (smještene iznad operativnog sustava) i hibridne hipervizore.
	Sustavi za izolirano izvršavanje softverski su proizvodi s digitalnim elementima koji upravljaju izvršavanjem i životnim ciklusom spremnika koji rade na jednom domaćinskom operativnom sustavu kao izolirani procesi, pri čemu dodjeljuju resurse te omogućuju upravljanje i orkestraciju pojedinačnih spremnika. U kontekstu ove kategorije proizvoda spremnik je softversko okruženje za izvršavanje koje objedinjuje jednu ili više softverskih komponenti i njihove ovisnosti u jedan paket, što omogućuje njegov neovisan i konzistentan rad.
2. Vatrozidovi, sustavi za otkrivanje i sprečavanje neovlaštenih upada	Vatrozidovi su proizvodi s digitalnim elementima koji štite povezanu mrežu ili sustav od neovlaštenog pristupa tako što prate i ograničavaju podatkovni komunikacijski promet prema toj mreži i iz nje. Kategorija obuhvaća, među ostalim, mrežne vatrozidove i vatrozidove za aplikacije kao što su vatrozidovi za internetske aplikacije ili filtri i pristupnici protiv neželjene e-pošte.
	Sustavi za otkrivanje neovlaštenih upada su proizvodi s digitalnim elementima koji praćenjem prometa od njegova ulaska u mrežno okruženje traže sumnjive aktivnosti kako bi otkrili ili utvrdili pokušaj neovlaštenog upada u povezanu mrežu ili sustav ili neovlašteni upad u tijeku ili neovlašteni upad koji se dogodio. Kategorija obuhvaća, među ostalim, sustave za otkrivanje neovlaštenih upada u mreži i sustave za otkrivanje neovlaštenih upada na lokalnom računalu.
	Sustavi za sprečavanje neovlaštenih upada su proizvodi s digitalnim elementima koji se sastoje od sustava za otkrivanje neovlaštenih upada koji aktivno reagira na neovlašteni upad u povezanu mrežu ili sustav. Kategorija obuhvaća, među ostalim, sustave za sprečavanje neovlaštenih upada u mreži i sustave za sprečavanje neovlaštenih upada na lokalnom računalu.

Kategorija proizvoda	Tehnički opis
3. Mikroprocesori otporni na manipuliranje	Proizvodi s digitalnim elementima koji su mikroprocesori sa sigurnosnim funkcionalnostima iz tablice „I. razred” točke 13. ovog Priloga, što uključuje dokaze za, otpornost ili odgovor na manipuliranje, i koji su uz to projektirani da pružaju zaštitu 2. ili 3. razine AVA_VAN, kako je utvrđeno u zajedničkim kriterijima i zajedničkoj evaluacijskoj metodologiji.
4. Mikrokontroleri otporni na manipuliranje	Proizvodi s digitalnim elementima koji su mikrokontroleri sa sigurnosnim funkcionalnostima iz tablice „I. razred” točke 14. ovog Priloga, što uključuje dokaze za, otpornost ili odgovor na manipuliranje, i koji su uz to projektirani da pružaju razinu zaštite AVA_VAN 2 ili 3, kako je utvrđeno u zajedničkim kriterijima i zajedničkoj evaluacijskoj metodologiji.

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

PRILOG II.

KRITIČNI PROIZVODI S DIGITALNIM ELEMENTIMA

Kategorija proizvoda	Tehnički opis
1. Hardverski uređaji sa sigurnosnim kutijama	Hardverski proizvodi s digitalnim elementima koji sigurno pohranjuju ili obrađuju osjetljive podatke ili upravljaju njima ili obavljaju kriptografske operacije te se sastoje od više zasebnih komponenti s hardverskim fizičkim omotačem koji kao protumjere protiv fizičkih napada daje dokaze za, otpornost ili odgovor na manipuliranje. Kategorija obuhvaća, među ostalim, fizičke terminale za plaćanje, hardverske sigurnosne module koji generiraju kriptografske elemente i upravljaju njima te tahografe koji odgovaraju navedenom opisu.
2. Pristupnici pametnih brojila u okviru pametnih sustava mjerenja kako su definirani u članku 2. točki 23. Direktive (EU) 2019/944 Europskog parlamenta i Vijeća ([1]) i drugi uređaji za napredne sigurnosne svrhe, među ostalim za sigurnu kriptoobradu	Pristupnici pametnih brojila proizvodi su s digitalnim elementima koji kontroliraju komunikaciju između komponenata pametnih sustava mjerenja, kako su definirani u članku 2. točki 23. Direktive (EU) 2019/944, ili komponenata povezanih s njima i ovlaštenih trećih strana, kao što su pružatelji energetskih usluga. Pristupnici pametnih brojila prikupljaju, obrađuju i pohranjuju podatke brojila ili osobne podatke, štite protoke podataka i informacija tako što podržavaju specifične kriptografske zahtjeve kao što su šifriranje i dešifriranje podataka, uključuju funkcije vatrozida i omogućavaju nadzor nad drugim uređajima. Kategorija obuhvaća, među ostalim, pristupnike pametnih brojila povezane s pametnim sustavima mjerenja električne energije kako su definirani u članku 2. točki 23. Direktive (EU) 2019/944. Može uključivati i pristupnike pametnih brojila koji se koriste u drugim pametnim sustavima mjerenja potrošnje drugih izvora energije kao što su plin ili toplina, pod uvjetom da pristupnik odgovara navedenom opisu.
3. Pametne kartice ili slični uređaji, uključujući sigurne elemente	Sigurni elementi su mikrokontroleri ili mikroprocesori s funkcijama povezanima sa sigurnošću, što uključuje dokaze za, otpornost ili odgovor na manipuliranje. Obično pohranjuju ili obrađuju kriptografske operacije ili osjetljive podatke ili upravljaju njima, primjerice identifikacijske vjerodajnice ili vjerodajnice za plaćanje. Sigurni elementi projektirani su tako da pružaju zaštitu barem razine AVA_VAN 4, kako je utvrđeno u zajedničkim kriterijima ili zajedničkoj evaluacijskoj metodologiji. To mogu biti zasebni silicijski elementi ili mogu biti integrirani u sustave na čipu (SoC). Sigurni elementi mogu uključivati aplikacijsko okruženje ili operativni sustav te jednu ili više aplikacija. Kategorija obuhvaća, među ostalim, module u skladu sa standardom TPM i ugrađene UICC kartice.
	Pametne kartice ili slični uređaji sigurni su elementi integrirani u noseći materijal, kao što je plastika ili drvo, u obliku kartice ili u drugim oblicima. Kategorija obuhvaća, među ostalim, osobne i putne isprave, kartice za kvalificirani potpis, zamjenjive UICC-ove, fizičke platne kartice, fizičke pristupne kartice, digitalne tahografske kartice ili narukvice s integriranim sigurnim elementima za plaćanje.

([1]) Direktiva (EU) 2019/944 Europskog parlamenta i Vijeća od 5. lipnja 2019. o zajedničkim pravilima za unutarnje tržište električne energije i izmjeni Direktive 2012/27/EU (SL L 158, 14.6.2019., str. 125., ELI: http://data.europa.eu/eli/dir/2019/944/oj).