2024/482

7.2.2024.

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)

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (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) ([1]), a posebno njezin članak 49. stavak 7.,

budući da:

(1) Ovom se Uredbom utvrđuju uloge, pravila i obveze i struktura europskog programa kibernetičkosigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) u skladu s europskim okvirom za kibernetičkosigurnosnu certifikaciju utvrđenim u Uredbi (EU) 2019/881. Osnova EUCC-a je Sporazum o uzajamnom priznavanju certifikata o sigurnosti informacijske tehnologije Skupine viših dužnosnika za sigurnost informacijskih sustava ([2]) („SOG-IS”) korištenjem zajedničkih kriterija, uključujući postupke i dokumente skupine.

(2) Program bi se trebao temeljiti na postojećim međunarodnim normama. Zajednički kriteriji su međunarodna norma za evaluaciju informacijske sigurnosti i objavljeni su npr. kao norma ISO/IEC 15408 Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti – Kriteriji za vrednovanje sigurnosti IT-a. Temelje se na evaluaciji koju obavlja treća strana i u njima je predviđeno sedam jamstvenih razina evaluacije (EAL). Uz zajedničke kriterije dolazi zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije objavljena npr. kao norma ISO/IEC 18045 – Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti – Kriteriji za vrednovanje sigurnosti IT-a – Metodologija za vrednovanje sigurnosti IT-a. U specifikacijama i dokumentima koji služe za primjenu odredbi ove Uredbe može se upućivati na javno dostupnu normu koje odgovara normi koja se koristi za certifikaciju na temelju ove Uredbe, kao što su zajednički kriteriji za evaluaciju sigurnosti informacijske tehnologije i zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije

(3) U EUCC-u se koriste komponente od 1 do 5 porodice po analizi ranjivosti u skladu sa zajedničkim kriterijima (AVA_VAN). Sve glavne odrednice i ovisnosti za analiziranje ranjivosti IKT proizvoda sadržane su u tih pet komponenti. Budući da komponente odgovaraju jamstvenim razinama iz ove Uredbe, one služe za razložan odabir te razine na temelju evaluacija sigurnosnih zahtjeva i rizika povezanog s namjenom IKT proizvoda. Podnositelj zahtjeva za EUCC certifikat trebao bi predočiti dokumentaciju o namjeni IKT proizvoda i analizu razina rizika povezanih s njom kako bi tijelo za ocjenjivanje sukladnosti moglo evaluirati primjerenost odabrane jamstvene razine. Ako evaluacijske i certifikacijske aktivnosti izvodi isto tijelo za ocjenjivanje sukladnosti, podnositelj zahtjeva trebao bi tražene informacije dostaviti samo jedanput.

(4) Tehnička domena je referentni okvir koji obuhvaća skupinu IKT proizvoda sa specifičnom i sličnom sigurnosnom funkcionalnosti za ublažavanje napada koji dijele karakteristike dane jamstvene razine. Tehnička domena sadržava specifikacije najsuvremenijih tehnika u kojima se opisuju specifični sigurnosni zahtjevi i dodatne evaluacijske metode, tehnike i alati koji se primjenjuju za certifikaciju IKT proizvoda u toj tehničkoj domeni. Dakle, tehnička domena također potiče usklađivanje evaluacije obuhvaćenih IKT proizvoda. Za certifikaciju na razinama

([1]) SL L 151, 7.6.2019., str. 15.

([2]) Sporazum o uzajamnom priznavanju certifikata o evaluaciji sigurnosti informacijske tehnologije, verzija 3.0 iz siječnja 2010., dostupan na sogis.eu, koji je odobrila Skupina viših dužnosnika za sigurnost informacijskih sustava Europske komisije kao odgovor na točku 3. Preporuke Vijeća 95/144/EZ od 7. travnja 1995. o zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije (SL L 93, 26.4.1995., str. 27.).

AVA_VAN.4 i AVA_VAN.5 trenutačno se uvelike koriste dvije tehničke domene. Prva je tehnička domena „pametne kartice i slični uređaji”, u kojoj znatni dijelovi zahtijevane sigurnosne funkcionalnosti ovise o specifičnim, namjenski prilagođenim i često odvojivim hardverskim elementima (npr. hardver pametne kartice, integrirani sklopovi, složeni proizvodi s pametnim karticama, moduli u skladu sa standardom TPM (*Trusted Platform Module*) u kontekstu tehnologije Trusted Computing, digitalne tahografske kartice). Druga je tehnička domena „hardverski uređaji sa sigurnosnom kutijom”, u kojoj znatan dio zahtijevane sigurnosne funkcionalnosti ovisi o hardverskom fizičkom omotaču (koji se naziva „sigurnosna kutija”) namijenjenom za obranu od izravnih napada, npr. terminali za plaćanje, tahografske jedinice u vozilima, pametna brojila, terminali za kontrolu pristupa i hardverski sigurnosni moduli).

(5) Pri podnošenju zahtjeva za certifikaciju podnositelj bi trebao svoje razloge za odabir jamstvene razine povezati s ciljevima iz članka 51. Uredbe (EU) 2019/881 i s odabirom komponenata iz kataloga sigurnosnih funkcionalnih zahtjeva i zahtjeva za sigurnosno jamstvo u zajedničkim kriterijima. Certifikacijska tijela trebala bi procijeniti primjerenost odabrane jamstvene razine i pobrinuti se da je odabrana razina razmjerna razini rizika povezanog s namjenom IKT proizvoda.

(6) Prema zajedničkim kriterijima certifikacija se radi s obzirom na potrebnu sigurnost koja obuhvaća definiciju sigurnosnog problema IKT proizvoda i sigurnosne ciljeve na temelju kojih se rješava sigurnosni problem. Sigurnosni problem sadržava pojedinosti o namjeni IKT proizvoda i s njom povezanim rizicima. Odabrani skup sigurnosnih zahtjeva odnosi se na sigurnosni problem i sigurnosne ciljeve IKT proizvoda.

(7) Profili zaštite su djelotvoran način da se unaprijed odrede zajednički kriteriji koji se primjenjuju na danu kategoriju IKT proizvoda, a stoga i bitan element u certifikaciji IKT proizvoda s određenim profilom zaštite. Profil zaštite koristi se za procjenu budućih potrebnih sigurnosti koje spadaju u kategoriju IKT proizvoda na koju se profil odnosi. Zahvaljujući njima postupak certifikacije IKT proizvoda je jednostavniji i učinkovitiji, a korisnici mogu lakše točno i precizno odrediti funkcionalnost IKT proizvoda. Profile zaštite stoga bi trebalo smatrati sastavnim dijelom IKT procesa koji vodi do certifikacije IKT proizvoda.

(8) Da bi profili zaštite mogli služiti u IKT procesu koji podupire razvoj i isporuku certificiranog IKT proizvoda, trebalo bi ih se moći certificirati neovisno o certifikaciji određenog IKT proizvoda obuhvaćenog odgovarajućim profilom zaštite. Zbog toga je profile zaštite bitno podvrgnuti barem istoj razini kontrole kao potrebnu sigurnost da bi se postigao visok stupanj kibernetičke sigurnosti. Profile zaštite trebalo bi evaluirati i certificirati odvojeno od s njima povezanog IKT proizvoda i isključivo primjenom jamstvenog razreda za profile zaštite (APE) i, prema potrebi, za konfiguracije profila zaštite (ACE) iz zajedničkih kriterija i zajedničke evaluacijske metodologije. Budući da su ti profili kao referentne vrijednosti u certifikaciji IKT proizvoda važni i osjetljivi, trebala bi ih certificirati samo javna tijela ili certifikacijsko tijelo koje je od nacionalnog tijela za kibernetičkosigurnosnu certifikaciju dobilo prethodno odobrenje za određeni profil zaštite. Zbog njihove temeljne važnosti za certifikaciju na visokoj jamstvenoj razini, osobito izvan tehničkih domena, profili zaštite trebali bi se sastavljati kao specifikacije najsuvremenijih tehnika koje bi trebala podržati Europska skupina za kibernetičkosigurnosnu certifikaciju (ECCG).

(9) Certificirane profile zaštite trebalo bi uključiti u praćenje sukladnosti i poštovanja obveza koje u okviru EUCC-a provode nacionalna tijela za kibernetičkosigurnosnu certifikaciju. Ako za određene certificirane profile zaštite postoje metodologija, alati i vještine koji se primjenjuju na pristupe evaluaciji IKT proizvoda, tehničke domene mogu se temeljiti na tim profilima zaštite.

(10) Kako bi se postiglo visoko povjerenje u certificirane IKT proizvode i visoko jamstvo njihove sigurnosti, u skladu s ovom Uredbom ne bi trebalo biti dopušteno samoocjenjivanje. Dopušteno bi trebalo biti samo ocjenjivanje sukladnosti koje provode treće strane, i to ITSEF i certifikacijska tijela.

(11) Zajednica SOG-IS dala je zajednička tumačenja i pristupe za primjenu zajedničkih kriterija i zajedničke evaluacijske metodologije u certifikaciji, osobito za visoku jamstvenu razinu koja se nastoji postići u tehničkim domenama „pametne kartice i slični uređaji” i „hardverski uređaji sa sigurnosnim kutijama”. Preuzimanjem takvih popratnih dokumenata u EUCC zajamčio bi se uredan prelazak s nacionalnih programa uvedenih u okviru SOG-IS-a na usklađeni europski program. Stoga bi u ovu Uredbu trebalo uključiti usklađene evaluacijske metodologije od opće važnosti za sve certifikacijske aktivnosti. Usto, Komisija bi trebala moći zatražiti od Europske skupine za kibernetičkosigurnosnu certifikaciju da donese mišljenje kojim se podržava i preporučuje primjena evaluacijskih metodologija navedenih u specifikacijama najsuvremenijih tehnika za certifikaciju IKT proizvoda ili profila zaštite u okviru EUCC-a. Stoga se u Prilogu I. u ovoj Uredbi navode specifikacije najsuvremenijih tehnika za evaluacijske aktivnosti tijela za ocjenjivanje sukladnosti. Europska skupina za kibernetičkosigurnosnu certifikaciju trebala bi podržati i održavati specifikacije najsuvremenijih tehnika. U certifikacijama bi trebalo koristiti specifikacije najsuvremenijih tehnika. Tijelo za ocjenjivanje sukladnosti nije ih obvezno koristiti samo u iznimnim i propisno opravdanim slučajevima i podložno određenim uvjetima, prije svega odobrenju nacionalnog tijela za kibernetičkosigurnosnu certifikaciju.

(12) Certifikacija IKT proizvoda na razini AVA_VAN 4 ili 5 trebala bi biti moguća samo pod specifičnim uvjetima i ako je dostupna specifična evaluacijska metodologija. Specifičnu evaluacijsku metodologiju mogu sadržavati specifikacije najsuvremenijih tehnika relevantne za tehničku domenu ili specifični profili zaštite utvrđeni u obliku specifikacije najsuvremenijih tehnika relevantne za predmetnu kategoriju proizvoda. Certifikacija na tim jamstvenim razinama trebala bi biti moguća samo u iznimnim i propisno opravdanim slučajevima, podložno specifičnim uvjetima, prije svega odobrenju, među ostalim i primjenjive evaluacijske metodologije, nacionalnog tijela za kibernetičkosigurnosnu certifikaciju. Takvi iznimni i propisno opravdani slučajevi mogu postojati ako se na temelju propisa Unije ili nacionalnih propisa zahtijeva certifikacija IKT proizvoda na razini AVA_VAN 4 ili 5. U iznimnim i propisno opravdanim slučajevima profili zaštite mogu se certificirati bez primjene relevantnih specifikacija najsuvremenijih tehnika, podložno posebnim uvjetima, prije svega odobrenju, među ostalim i primjenjive evaluacijske metodologije, nacionalnog tijela za kibernetičkosigurnosnu certifikaciju.

(13) Svrha znakova i oznaka koje se upotrebljavaju u okviru EUCC-a je da korisnicima vidljivo dokažu vjerodostojnost certificiranog IKT proizvoda korisnicima i omoguće im da kupuju IKT proizvode na temelju informacija u njima. Znakovi i oznake trebali bi se koristiti u skladu s pravilima i uvjetima iz norme ISO/IEC 17065 i, prema potrebi, ISO/IEC 17030 i odgovarajućim uputama iz te norme.

(14) Certifikacijska tijela trebala bi odlučivati o razdoblju valjanosti certifikata uzimajući u obzir životni ciklus IKT proizvoda u pitanju. Razdoblje valjanosti ne bi trebalo biti dulje od pet godina. Nacionalna tijela za kibernetičkosigurnosnu certifikaciju trebala bi raditi na usklađivanju razdoblja valjanosti u Uniji.

(15) Ako se opseg postojećeg EUCC certifikata smanji, trebalo bi ga povući pa izdati novi certifikat s novim opsegom kako bi korisnici bili jasno informirani o trenutačnom opsegu i jamstvenoj razini certifikata za određeni IKT proizvod.

(16) Certifikacija profila zaštite razlikuje se od certifikacije IKT proizvoda jer se odnosi na IKT proces. Budući da se profil zaštite odnosi na kategoriju IKT proizvoda, njegova evaluacija i certifikacija ne mogu se provoditi na temelju jednog IKT proizvoda. Budući da su u profilu zaštite objedinjeni opći sigurnosni zahtjevi za kategoriju IKT proizvoda i da profil ne ovisi o tome u kojem je obliku je opskrbljivač izradio IKT proizvod, razdoblje valjanosti EUCC certifikata za profil zaštite u načelu bi trebalo biti najmanje pet godina s mogućnošću produljenja do kraja životnog vijeka tog profila.

(17) Tijelo za ocjenjivanje sukladnosti definirano je kao tijelo koje obavlja poslove ocjenjivanja sukladnosti uključujući umjeravanje, ispitivanje, certifikaciju i pregled. Kako bi kvaliteta usluga bila visoka, u ovoj se Uredbi određuje da bi aktivnosti ispitivanja s jedne strane i aktivnosti certifikacije i pregleda s druge strane trebali provoditi međusobno neovisni subjekti, točnije centri za evaluaciju sigurnosti informacijske tehnologije („ITSEF”) odnosno certifikacijska tijela. Obje vrste tijela za ocjenjivanje sukladnosti trebale bi biti akreditirane i, u određenim situacijama, autorizirane.

(18) Nacionalno akreditacijsko tijelo trebalo bi akreditirati certifikacijsko tijelo za znatnu i visoku jamstvenu razinu u skladu s normom ISO/IEC 17065. Uz to što bi trebala biti akreditirana u skladu s Uredbom (EU) 2019/881 u vezi s Uredbom (EZ) br. 765/2008 tijela za ocjenjivanje sukladnosti trebala bi ispunjavati posebne zahtjeve kako bi se zajamčila njihova tehnička kompetentnost za evaluaciju kibernetičkosigurnosnih zahtjeva za visoku jamstvenu razinu EUCC-a, što se potvrđuje „autorizacijom". Kao potporu postupku autorizacije, trebalo bi sastaviti relevantne specifikacije najsuvremenijih tehnika, koje, nakon što ih podrži Europska skupina za kibernetičkosigurnosnu certifikaciju, treba objaviti ENISA.

(19) Tehničku kompetentnost ITSEF-a trebalo bi ocijeniti akreditacijom laboratorija za ispitivanje u skladu s normom ISO/IEC 17025, dopunjenu normom ISO/IEC 23532-1, za cijeli skup evaluacijskih aktivnosti relevantnih za jamstvenu razinu i navedenih u normi ISO/IEC 18045 u vezi s normom ISO/IEC 15408. Certifikacijsko tijelo i ITSEF trebali bi uspostaviti i održavati odgovarajući sustav upravljanja kompetencijama osoblja koji se temelji na normi ISO/IEC 19896-1 za elemente i razine stručnosti te za procjenu stručnosti. Zahtjevi koji se primjenjuju za razinu znanja, vještina, iskustva i obrazovanja evaluatora trebali bi se temeljiti na normi ISO/IEC 19896-3. U slučaju odstupanja od takvih sustava upravljanja kompetencijama trebalo bi u skladu s ciljevima sustava dokazati ekvivalentnost tih odredbi i mjera.

(20) Da bi dobio autorizaciju, ITSEF bi trebao dokazati da je sposoban utvrditi da nema poznatih ranjivosti, da su najsuvremenije sigurnosne funkcionalnosti tehnologije u pitanju ispravno i dosljedno implementirane i da je ciljani IKT proizvod otporan na umješne napadače. Za autorizacije u tehničkoj domeni „pametne kartice i slični uređaji" ITSEF bi uz to trebao dokazati i tehničke sposobnosti potrebne za evaluacijske aktivnosti i s njima povezane zadaće definirane u popratnom dokumentu zajedničkih kriterija „Minimalni zahtjevi za ITSEF u pogledu sigurnosnih evaluacija pametnih kartica i sličnih uređaja" ([3]). Za autorizaciju u tehničkoj domeni „hardverski uređaji sa sigurnosnim kutijama" ITSEF bi uz to trebao dokazati da ispunjava minimalne tehničke zahtjeve potrebne za obavljanje evaluacijskih aktivnosti i s njima povezanih zadaća na hardverskim uređajima sa sigurnosnim kutijama u skladu s preporukom Europske skupine za kibernetičkosigurnosnu certifikaciju. U kontekstu minimalnih zahtjeva ITSEF bi trebao biti sposoban izvoditi različite vrste napada navedene u popratnom dokumentu zajedničkih kriterija „Primjena potencijala napada na hardverske uređaje sa sigurnosnim kutijama". Te sposobnosti obuhvaćaju znanje i vještine evaluatora te opremu i evaluacijske metode potrebne za utvrđivanje i procjenjivanje različitih vrsta napada.

(21) Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju trebalo bi pratiti kako certifikacijska tijela, ITSEF i nositelji certifikata ispunjavaju svoje obveze koje proizlaze iz ove Uredbe i Uredbe (EU) 2019/881. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju trebalo bi u tu svrhu upotrebljavati sve odgovarajuće izvore informacija, što uključuje informacije od sudionika u postupku certifikacije i iz vlastitih istraga.

(22) Certifikacijska tijela trebala bi surađivati s relevantnim tijelima za nadzor tržišta i uzeti u obzir svaku informaciju o ranjivostima koja bi mogla biti relevantna za IKT proizvode za koje su izdala certifikate. Certifikacijska tijela trebala bi pratiti profile zaštite koje su certificirala kako bi ustanovila jesu li sigurnosni zahtjevi utvrđeni za određenu kategoriju IKT proizvoda primjereni trenutačnom stanju prijetnji.

(23) Kao potporu praćenju poštovanja obveza nacionalna tijela za kibernetičkosigurnosnu certifikaciju trebala bi surađivati s relevantnim tijelima za nadzor tržišta u skladu s člankom 58. Uredbe (EU) 2019/881 i Uredbom (EU) 2019/1020 Europskog parlamenta i Vijeća ([4]). Gospodarski subjekti u Uniji obvezni su dijeliti informacije i surađivati s tijelima za nadzor tržišta u skladu s člankom 4. stavkom 3. Uredbe (EU) 2019/1020.

([3]) Biblioteka za jedinstveno tumačenje: Minimalni zahtjevi za ITSEF u pogledu sigurnosnih evaluacija pametnih kartica i sličnih uređaja (*Joint Interpretation Library: Minimum ITSEF Requirements for Security Evaluations of Smart cards and similar devices*), verzija 2.1 iz veljače 2020., dostupno na sogis.eu.

([4]) Uredba (EU) 2019/1020 Europskog parlamenta i Vijeća od 20. lipnja 2019. o nadzoru tržišta i sukladnosti proizvoda i o izmjeni Direktive 2004/42/EZ i uredbi (EZ) br. 765/2008 i (EU) br. 305/2011 (SL L 169, 25.6.2019., str. 1.).

(24) Certifikacijska tijela trebala bi pratiti poštovanje obveza nositelja certifikata i sukladnost svih certifikata izdanih u okviru EUCC-a. Praćenje bi trebalo zajamčiti da se sva ITSEF-ova izvješća o evaluaciji i njihovi zaključci te evaluacijski kriteriji i metode dosljedno i ispravno primjenjuju u svim certifikacijskim aktivnostima.

(25) Ako se otkriju potencijalne nesukladnosti koje utječu na certificirani IKT proizvod, važno je da reakcija bude razmjerna. Stoga se certifikati mogu suspendirati. Suspenzija bi trebala uključivati određena ograničenja promidžbe i upotrebe tog IKT proizvoda, ali ne bi trebala utjecati na valjanost certifikata. Nositelj EU certifikata trebao bi o suspenziji obavijestiti kupce IKT proizvoda na koji se suspenzija odnosi, a relevantna nacionalna tijela za kibernetičkosigurnosnu certifikaciju trebala bi obavijestiti relevantna tijela za nadzor tržišta. Da bi se obavijestila javnost, ENISA bi informacije o suspenziji trebala objaviti na namjenskoj internetskoj stranici.

(26) Nositelj EUCC certifikata trebao bi uvesti potrebne postupke za upravljanje ranjivostima i pobrinuti se da ti postupci budu sastavni dio njegove organizacije. Nositelj EUCC certifikata trebao bi provesti analizu utjecaja ranjivosti čim postane svjestan moguće ranjivosti. Utvrdi li se analizom utjecaja ranjivosti da se ranjivost može iskoristiti, nositelj certifikata trebao bi poslati izvješće o procjeni certifikacijskom tijelu, koje bi onda o tome trebalo obavijestiti nacionalno tijelo za kibernetičkosigurnosnu certifikaciju. Izvješće bi trebalo sadržavati informacije o posljedicama ranjivosti, potrebnim promjenama ili korektivnim rješenjima, uključujući moguće šire posljedice ranjivosti i korektivna rješenja za druge proizvode. Prema potrebi, postupak obavješćivanja o ranjivostima trebao bi biti dopunjen normom EN ISO/IEC 29147.

(27) Za potrebe certifikacije tijela za ocjenjivanje sukladnosti i nacionalna tijela za kibernetičkosigurnosnu certifikaciju prikupljaju povjerljive i osjetljive podatke i poslovne tajne, među ostalim i o intelektualnom vlasništvu ili praćenju poštovanja obveza, za koje je potrebna odgovarajuća zaštita. Ta bi tijela stoga trebala imati potrebne tehničke kompetencije i znanje te uspostaviti sustave za zaštitu informacija. Zahtjevi i uvjeti za zaštitu informacija trebali bi biti ispunjeni i za akreditaciju i za autorizaciju.

(28) ENISA bi na svojim internetskim stranicama o kibernetičkosigurnosnoj certifikaciji trebala objaviti popis certificiranih profila zaštite s njihovim statusom u skladu s Uredbom (EU) 2019/881.

(29) Ovom se Uredbom utvrđuju uvjeti za sporazume o uzajamnom priznavanju s trećim zemljama. Takvi sporazumi o uzajamnom priznavanju mogu biti bilateralni ili multilateralni i trebali bi zamijeniti slične sporazume koji su trenutačno na snazi. Kako bi se lakše prešlo na takve sporazume o uzajamnom priznavanju, države članice mogu određeno vrijeme nastaviti primjenjivati postojeće dogovore o suradnji s trećim zemljama.

(30) Certifikacijska tijela koja izdaju EUCC certifikate visoke jamstvene razine, kao i relevantni, s njima povezani ITSEF-ovi, trebali bi proći istorazinsko ocjenjivanje. Cilj istorazinskog ocjenjivanja trebao bi biti utvrđivanje kontinuirane sukladnosti ustroja i postupaka certifikacijskog tijela koje se istorazinski ocjenjuje sa zahtjevima EUCC-a. To istorazinsko ocjenjivanje nije istorazinsko ocjenjivanje među nacionalnim tijelima za kibernetičkosigurnosnu certifikaciju, kako je utvrđeno u članku 59. Uredbe (EU) 2019/881. Istorazinskim ocjenjivanjem trebalo bi potvrditi da certifikacijska tijela rade na usklađen način i da proizvode istu kvalitetu certifikata te bi trebalo utvrditi sve potencijalne prednosti ili nedostatke u radu certifikacijskih tijela, među ostalim u cilju razmjene primjera dobre prakse. Budući da postoje različite vrste certifikacijskih tijela, trebalo bi dopustiti različite vrste istorazinskih ocjenjivanja. U složenijim slučajevima, npr. kad certifikacijska tijela izdaju certifikate različitih razina AVA_VAN, mogu se upotrebljavati različite vrste istorazinskih ocjenjivanja, pod uvjetom da su svi zahtjevi ispunjeni.

(31) Europska skupina za kibernetičkosigurnosnu certifikaciju trebala bi imati važnu ulogu u održavanju programa. Trebala bi ga, među ostalim, provoditi u suradnji s privatnim sektorom, osnivanjem specijaliziranih podskupina i obavljanjem relevantnog pripremnog rada i pružanjem pomoći koje zatraži Komisija. Europska skupina za kibernetičkosigurnosnu certifikaciju ima važnu ulogu u potvrđivanju specifikacija najsuvremenijih tehnika. U potvrđivanju i donošenju specifikacija najsuvremenijih tehnika trebalo bi uzeti u obzir elemente iz članka 54. stavka 1. točke (c) Uredbe (EU) 2019/881. Tehničke domene i specifikacije najsuvremenijih tehnika trebalo bi

objaviti u Prilogu I. ovoj Uredbi. Profile zaštite koji su doneseni kao specifikacije najsuvremenijih tehnika trebalo bi objaviti u Prilogu II. Kako bi se ti prilozi mogli mijenjati prema potrebi, Komisija ih može mijenjati u skladu s postupkom utvrđenim u članku 66. stavku 2. Uredbe (EU) 2019/881 uz uzimanje u obzir mišljenja Europske skupine za kibernetičkosigurnosnu certifikaciju. Prilog III. sadržava preporučene profile zaštite koji u trenutku stupanja na snagu ove Uredbe nisu specifikacije najsuvremenijih tehnika. Trebalo bi ih objaviti na internetskim stranicama ENISA-e iz članka 50. stavka 1. Uredbe (EU) 2019/881.

(32) Ova bi se Uredba trebala početi primjenjivati 12 mjeseci nakon stupanja na snagu. Za zahtjeve iz poglavlja IV. i Priloga V. nije potrebno prijelazno razdoblje pa bi se oni trebali primjenjivati od stupanja na snagu ove Uredbe.

(33) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Europskog odbora za kibernetičkosigurnosnu certifikaciju osnovanog člankom 66. Uredbe (EU) 2019/881,

DONIJELA JE OVU UREDBU:

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet i područje primjene

Ovom se Uredbom utvrđuje europski program kibernetičkosigurnosne certifikacije temeljen na zajedničkim kriterijima (EUCC).

Ova se Uredba primjenjuje na sve proizvode informacijskih i komunikacijskih tehnologija („IKT”), uključujući njihovu dokumentaciju, koji se podnose na certifikaciju na temelju EUCC-a te na sve profile zaštite koji se podnose na certifikaciju u okviru IKT procesa čiji je krajnji cilj certifikacija IKT proizvoda.

Članak 2.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „zajednički kriteriji” znači zajednički kriteriji za evaluaciju sigurnosti informacijske tehnologije kako su utvrđeni u normi ISO/IEC 15408;

2. „zajednička evaluacijska metodologija” znači zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije kako je utvrđena u normi ISO/IEC 18045;

3. „predmet evaluacije” znači IKT proizvod ili njegov dio, ili profil zaštite kao dio IKT procesa, nad kojim se provodi evaluacija kibernetičke sigurnosti radi izdavanja EUCC certifikata;

4. „potrebna sigurnost” znači izjava o implementacijski ovisnim sigurnosnim zahtjevima za određeni IKT proizvod;

5. „profil zaštite” znači IKT proces kojim se utvrđuju sigurnosni zahtjevi za određenu kategoriju IKT proizvoda s obzirom na implementacijski neovisne sigurnosne potrebe i koji može služiti za ocjenjivanje IKT proizvoda iz te kategorije u svrhu njihove certifikacije;

6. „tehničko izvješće o evaluaciji” znači dokument koji sastavlja ITSEF kako bi iznio rezultate, sudove i obrazloženja iz evaluacije IKT proizvoda ili profila zaštite provedene u skladu s pravilima i obvezama utvrđenima u ovoj Uredbi;

7. „ITSEF” znači centar za evaluaciju sigurnosti informacijske tehnologije koji je tijelo za ocjenjivanje sukladnosti kako je definirano u članku 2. točki 13. Uredbe (EZ) br. 765/2008 koje obavlja evaluacijske zadaće;

8. „razina AVA_VAN” znači jamstvena razina analize ranjivosti koja označava stupanj aktivnosti evaluacije kibernetičke sigurnosti koje su provedene radi utvrđivanja razine otpornosti na potencijalnu iskoristivost nedostataka ili slabih točaka predmeta evaluacije u njegovu radnom okruženju kako je utvrđeno u zajedničkim kriterijima;

9. „EUCC certifikat” znači certifikat kibernetičke sigurnost izdan u okviru EUCC-a za IKT proizvode ili za profile zaštite koji se mogu upotrebljavati isključivo u IKT postupku certifikacije IKT proizvoda;

10. „složeni proizvod” znači IKT proizvod koji se evaluira zajedno s drugim osnovnim IKT proizvodom kojem je već izdan EUCC certifikat i o čijoj sigurnosnoj funkcionalnosti taj složeni IKT proizvod ovisi;

11. „nacionalno tijelo za kibernetičkosigurnosnu certifikaciju” znači tijelo koje je imenovala država članica na temelju članka 58. stavka 1. Uredbe (EU) 2019/881;

12. „certifikacijsko tijelo” znači tijelo za ocjenjivanje sukladnosti kako je definirano u članku 2. točki 13. Uredbe (EZ) br. 765/2008 koje obavlja certifikacijske aktivnosti;

13. „tehnička domena” znači zajednički tehnički okvir koji se odnosi na određenu tehnologiju namijenjen za usklađenu certifikaciju na temelju skupa karakterističnih sigurnosnih zahtjeva;

14. „specifikacija najsuvremenijih tehnika” znači dokument u kojem su navedene evaluacijske metode, tehnike i alati koje se primjenjuju na certifikaciju IKT proizvoda ili sigurnosne zahtjeve za generičku kategoriju IKT proizvoda ili bili koji drugi zahtjevi potrebni za certifikaciju te koji je namijenjen za usklađivanje evaluacija, osobito tehničkih domena ili profila zaštite;

15. „tijelo za nadzor tržišta” znači tijelo definirano u članku 3. točki 4. Uredbe (EU) 2019/1020.

Članak 3.

Evaluacijske norme

Za evaluacije u okviru EUCC-a vrijede sljedeće norme:

(a) zajednički kriteriji;

(b) zajednička evaluacijska metodologija.

Članak 4.

Jamstvene razine

1. Certifikacijska tijela izdaju EUCC certifikate sa znatnom ili visokom jamstvenom razinom.

2. Certifikati EUCC-a sa znatnom jamstvenom razinom odgovaraju certifikatima razine AVA_VAN 1 ili 2.

3. Certifikati EUCC-a s visokom jamstvenom razinom odgovaraju certifikatima razine AVA_VAN 3, 4 ili 5.

4. U jamstvenoj razini potvrđenoj u EUCC certifikatu mora se razlikovati sukladnu i proširenu primjenu jamstvenih komponenti kako je specificirano u zajedničkim kriterijima u skladu s Prilogom VIII.

5. Tijela za ocjenjivanje sukladnosti primjenjuju one jamstvene komponente o kojima ovisi odabrana razina AVA_VAN u skladu s normama iz članka 3.

Članak 5.

Metode certifikacije IKT proizvoda

1. Certifikacija IKT proizvoda provodi se s obzirom na njegovu potrebnu sigurnost:

(a) kako ju je definirao podnositelj zahtjeva; ili

(b) prema certificiranom profilu zaštite kao dijelu IKT procesa ako IKT proizvod pripada kategoriji IKT proizvoda obuhvaćenoj tim profilom zaštite.

2. Profili zaštite certificiraju se isključivo u svrhu certifikacije IKT proizvoda koji pripadaju određenoj kategoriji IKT proizvoda obuhvaćenih profilom zaštite.

Članak 6.

Samoocjenjivanje sukladnosti

Samoocjenjivanje sukladnosti u smislu članka 53. Uredbe (EU) 2019/881 nije dopušteno.

POGLAVLJE II.

CERTIFIKACIJA IKT PROIZVODA

ODJELJAK I.

Evaluacija: specifične norme i zahtjevi

Članak 7.

Kriteriji i metode za evaluaciju IKT proizvoda

1. IKT proizvod podnesen na certifikaciju evaluira se minimalno na temelju:

(a) primjenjivih elemenata normi iz članka 3.;

(b) razreda zahtjeva za sigurnosna jamstva za procjenu ranjivosti i neovisno funkcionalno testiranje, kako je utvrđeno u evaluacijskim normama iz članka 3.;

(c) razine rizika povezane s namjenom predmetnih IKT proizvoda u skladu s člankom 52. Uredbe (EU) 2019/881 i njihovim sigurnosnim funkcijama kojima se podupiru sigurnosni ciljevi iz članka 51. Uredbe (EU) 2019/881;

(d) primjenjivih specifikacija najsuvremenijih tehnika navedenih u Prilogu I.; i

(e) primjenjivih certificiranih profila zaštite navedenih u Prilogu II.

2. U iznimnim i propisno opravdanim slučajevima tijelo za ocjenjivanje sukladnosti može zatražiti da se suzdrži od primjene relevantne specifikacije najsuvremenijih tehnika. U takvim slučajevima tijelo za ocjenjivanje sukladnosti o tome šalje obavijest s obrazloženjem zahtjeva nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ocjenjuje obrazloženje iznimke i, ako je opravdana, odobrava je. Do donošenja odluke

nacionalnog tijela za kibernetičkosigurnosnu certifikaciju tijelo za ocjenjivanje sukladnosti ne smije izdati nikakav certifikat. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju o odobrenoj iznimci bez nepotrebne odgode obavješćuje Europsku skupinu za kibernetičkosigurnosnu certifikaciju, koja može izdati mišljenje. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju mora koliko je god moguće uzeti u obzir mišljenje Europske skupine za kibernetičkosigurnosnu certifikaciju.

3. Certifikacija IKT proizvoda na razini AVA_VAN 4 ili 5 moguća je samo u sljedećim scenarijima:

(a) ako je IKT proizvod obuhvaćen bilo kojom tehničkom domenom iz Priloga I., evaluira ga se u skladu s primjenjivim specifikacijama najsuvremenijih tehnika tih tehničkih domena;

(b) ako IKT proizvod pripada kategoriji IKT proizvoda obuhvaćenih certificiranim profilom zaštite koji uključuje razinu AVA_VAN 4 ili 5 i koji je u Prilogu II. naveden kao najsuvremeniji profil zaštite, evaluira ga se u skladu s evaluacijskom metodologijom određenom za taj profil zaštite,

(c) ako točke (a) i (b) ovog stavka nisu primjenjive i ako uključivanje tehničke domene u Prilog I. ili certificiranog profila zaštite u Prilog II. nije vjerojatno u doglednoj budućnosti, evaluira ga se podložno uvjetima utvrđenima u stavku 4. i to samo u iznimnim i propisno opravdanim slučajevima.

4. Ako tijelo za ocjenjivanje sukladnosti smatra da pred sobom ima iznimni i propisno opravdani slučaj iz stavka 3. točke (c), nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju šalje obavijest o planiranoj certifikaciji s obrazloženjem i predloženom evaluacijskom metodologijom. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ocjenjuje obrazloženje iznimke i, ako je opravdana, odobrava ili mijenja evaluacijsku metodologiju koju treba primijeniti tijelo za ocjenjivanje sukladnosti. Do donošenja odluke nacionalnog tijela za kibernetičkosigurnosnu certifikaciju tijelo za ocjenjivanje sukladnosti ne smije izdati nikakav certifikat. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju o planiranoj certifikaciji bez nepotrebne odgode izvješćuje Europsku skupinu za kibernetičkosigurnosnu certifikaciju, koja može izdati mišljenje. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju mora koliko je god moguće uzeti u obzir mišljenje Europske skupine za kibernetičkosigurnosnu certifikaciju.

5. Za IKT proizvod u postupku evaluacije složenog proizvoda u skladu s relevantnim specifikacijama najsuvremenijih tehnika ITSEF koji je proveo evaluaciju osnovnog IKT proizvoda daje relevantne informacije ITSEF-u koji provodi evaluaciju složenog IKT proizvoda.

ODJELJAK II.

IZDAVANJE, OBNAVLJANJE I POVLAČENJE EUCC CERTIFIKATA

Članak 8.

Informacije potrebne za certifikaciju

1. Podnositelj zahtjeva za certifikaciju na temelju EUCC-a certifikacijskom tijelu i ITSEF-u dostavlja ili na drugi način stavlja na raspolaganje sve informacije potrebne za certifikacijske aktivnosti.

2. Informacije iz stavka 1. uključuju sve relevantne dokaze u skladu s odjeljcima o „elementima koje su izradili razvojni inženjeri" u odgovarajućem formatu kako je utvrđen u odjeljcima o „sadržaju i prikazu elementa dokaza" iz zajedničkih kriterija i zajedničke evaluacijske metodologije za odabranu jamstvenu razinu i povezane zahtjeve za sigurnosno jamstvo. Dokazi prema potrebi uključuju detaljne podatke o IKT proizvodu i njegovu izvornom kodu u skladu s ovom Uredbom, uz primjenu zaštitnih mjera protiv neovlaštenog objavljivanja.

3. Podnositelji zahtjeva za certifikaciju mogu certifikacijskom tijelu dostaviti odgovarajuće rezultate evaluacije iz prethodne certifikacije na temelju:

(a) ove Uredbe;

(b) drugog europskog programa kibernetičkosigurnosne certifikacije donesenog na temelju članka 49. Uredbe (EU) 2019/881;

(c) nacionalnog programa iz članka 49. ove Uredbe.

4. Ako su rezultati evaluacije relevantni za njegove zadaće, ITSEF može iskoristiti postojeće rezultate evaluacije pod uvjetom da su ti rezultati u skladu s primjenjivim zahtjevima i da je potvrđena njihova vjerodostojnost.

5. Ako certifikacijsko tijelo dopusti certifikaciju proizvoda kao složenog proizvoda, podnositelj zahtjeva za certifikaciju certifikacijskom tijelu i ITSEF-u, prema potrebi, stavlja na raspolaganje sve potrebne elemente u skladu sa specifikacijom najsuvremenijih tehnika.

6. Podnositelji zahtjeva za certifikaciju certifikacijskom tijelu i ITSEF-u dostavljaju sljedeće informacije:

(a) poveznicu na svoje internetske stranice s dodatnim informacijama o kibernetičkoj sigurnosti iz članka 55. Uredbe (EU) 2019/881;

(b) opis postupaka podnositelja zahtjeva za upravljanje ranjivostima i obavješćivanje o ranjivostima.

7. Certifikacijsko tijelo, ITSEF i podnositelj zahtjeva dužni su svu relevantnu dokumentaciju iz ovog članka čuvati pet godina od isteka certifikata.

Članak 9.

Uvjeti za izdavanje EUCC certifikata

1. Certifikacijska tijela izdaju EUCC certifikat ako su ispunjeni svi sljedeći uvjeti:

(a) kategorija IKT proizvoda obuhvaćena je u akreditaciji i, ako je primjenjivo, autorizaciji certifikacijskog tijela i ITSEF-a koji sudjeluje u certifikaciji;

(b) podnositelj zahtjeva za certifikaciju potpisao je izjavu o preuzimanju svih obveza iz stavka 2.;

(c) ITSEF je bez prigovora dovršio evaluaciju na temelju evaluacijskih normi, kriteriji i metoda iz članaka 3. i 7.;

(d) certifikacijsko tijelo zaključilo je bez prigovora pregled rezultata evaluacije;

(e) certifikacijsko tijelo potvrdilo je da su tehnička izvješća o evaluaciji koja je dostavio ITSEF u skladu s dostavljenim dokazima te da su evaluacijske norme, kriteriji i metode ocjenjivanja iz članaka 3. i 7. pravilno primijenjeni.

2. Podnositelj zahtjeva za certifikaciju obvezuje se:

(a) certifikacijskom tijelu i ITSEF-u dostaviti sve potrebne potpune i točne informacije te, na zahtjev, dostaviti dodatne potrebne informacije;

(b) ne reklamirati IKT proizvod kao certificiran na temelju EUCC-a prije nego što EUCC certifikat bude izdan;

(c) reklamirati IKT proizvod kao certificiran samo u skladu s opsegom utvrđenim u EUCC certifikatu;

(d) u slučaju suspenzije, povlačenja ili isteka EUCC certifikata, odmah prestati reklamirati IKT proizvod kao certificiran;

(e) pobrinuti se da IKT proizvodi u prodaji za koje se ističe da posjeduju EUCC certifikat budu strogo istovjetni certificiranom IKT proizvodu;

(f) poštovati pravila o upotrebi znaka i oznake koji su uvedeni za EUCC certifikat u skladu s člankom 11.

3. Za IKT proizvod u postupku certifikacije složenog proizvoda u skladu s relevantnim specifikacijama najsuvremenijih tehnika certifikacijsko tijelo koje je provelo certifikaciju osnovnog IKT proizvoda daje relevantne podatke certifikacijskom tijelu koje provodi certifikaciju složenog IKT proizvoda.

Članak 10.

Sadržaj i format EUCC certifikata

1. EUCC certifikat mora sadržavati barem informacije utvrđene u Prilogu VII.

2. U EUCC certifikatu ili izvješću o certifikaciji moraju se nedvosmisleno navesti opseg i granice certificiranog IKT proizvoda te je li certificiran cijeli IKT proizvod ili samo njegovi dijelovi.

3. Certifikacijsko tijelo podnositelju zahtjeva izdaje EUCC certifikat barem u elektroničkom obliku.

4. Certifikacijsko tijelo sastavlja izvješće o certifikaciji u skladu s Prilogom V. za svaki EUCC certifikat koji izda. Izvješće o certifikaciji temelji se na tehničkom izvješću o evaluaciji koje izdaje ITSEF. U tehničkom izvješću o evaluaciji i izvješću o certifikaciji navode se specifični evaluacijski kriteriji i metode iz članka 7. koji su primijenjeni u evaluaciji.

5. Certifikacijsko tijelo nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju i ENISA-i u elektroničkom obliku dostavlja svaki EUCC certifikat i svako izvješće o certifikaciji.

Članak 11.

Znak i oznaka

1. Nositelj certifikata smije staviti znak i oznaku na certificirani IKT proizvod. Taj znak i oznaka su dokaz da je IKT proizvod certificiran u skladu s ovom Uredbom. Znak i oznaka stavljaju se u skladu s ovim člankom i Prilogom IX.

2. Znak i oznaka postavljeni na certificirani IKT proizvod ili njegovu pločicu s podacima moraju biti vidljivi, čitljivi i neizbrisivi. Ako to zbog prirode proizvoda nije moguće ili opravdano, stavljaju se na pakiranje i u popratne dokumente. Ako se certificirani IKT proizvod isporučuje u obliku softvera, znak i oznaka moraju biti vidljivi, čitljivi i neizbrisivi u njegovoj popratnoj dokumentaciji ili ta dokumentacija korisnicima mora biti lako i izravno dostupna na internetskim stranicama.

3. Znak i oznaka moraju biti u skladu s Prilogom IX. i sadržavati:

(a) jamstvenu razinu i razinu AVA_VAN certificiranog IKT proizvoda;

(b) jedinstvenu identifikacijsku oznaku certifikata koja se sastoji od:

1. imena programa;

2. imena i referentnog broja akreditacije certifikacijskog tijela koje je izdalo certifikat;

3. godine i mjeseca izdavanja;

4. identifikacijskog broja koji je dodijelilo certifikacijsko tijelo koje je izdalo certifikat.

4. Uz znak i oznaku mora biti prisutan QR kod s poveznicom na internetsku stranicu na kojoj su barem:

(a) podaci o valjanosti certifikata;

(b) nužni podaci o certifikaciji iz priloga V. i VII.;

(c) podaci koje je nositelj certifikata dužan objaviti u skladu s člankom 55. Uredbe (EU) 2019/881; i

(d) ako je primjenjivo, podaci iz evidencije koji se odnose na određene prijašnje certifikacije IKT proizvoda kako bi se omogućila sljedivost.

Članak 12.

Razdoblje valjanosti EUCC certifikata

1. Certifikacijsko tijelo određuje razdoblje valjanosti svakog izdanog EUCC certifikata uzimajući u obzir karakteristike certificiranog IKT proizvoda.

2. Razdoblje valjanosti EUCC certifikata ne smije biti dulje od pet godina.

3. Odstupajući od stavka 2., to razdoblje smije biti dulje od pet godina ako to prethodno odobri nacionalno tijelo za kibernetičkosigurnosnu certifikaciju. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju o dodijeljenom odobrenju bez nepotrebne odgode obavješćuje Europsku skupinu za kibernetičkosigurnosnu certifikaciju.

Članak 13.

Revizija EUCC certifikata

1. Na zahtjev nositelja certifikata ili iz drugih opravdanih razloga certifikacijsko tijelo može odlučiti revidirati EUCC certifikat za određeni IKT proizvod. Revizija se provodi u skladu s Prilogom IV. Opseg revizije određuje certifikacijsko tijelo. Ako je to potrebno radi revizije, certifikacijsko tijelo zahtijeva od ITSEF-a da provede ponovnu evaluaciju certificiranog IKT proizvoda.

2. Na temelju rezultata revizije i, prema potrebi, ponovne evaluacije, certifikacijsko tijelo:

(a) potvrđuje EUCC certifikat;

(b) povlači EUCC certifikat u skladu s člankom 14.;

(c) povlači EUCC certifikat u skladu s člankom 14. i izdaje novi EUCC certifikat s jednakim opsegom i produljenim razdobljem valjanosti; ili

(d) povlači EUCC certifikat u skladu s člankom 14. i izdaje novi EUCC certifikat s drukčijim opsegom.

3. Certifikacijsko tijelo može odlučiti da u skladu s člankom 30. bez nepotrebne odgode suspendira EUCC certifikat dok nositelj EUCC certifikata ne poduzme korektivne mjere.

Članak 14.

Povlačenje EUCC certifikata

1. Ne dovodeći u pitanje članak 58. stavak 8. točku (e) Uredbe (EU) 2019/881, EUCC certifikat povlači certifikacijsko tijelo koje je taj certifikat izdalo.

2. Certifikacijsko tijelo iz stavka 1. o povlačenju certifikata obavješćuje nacionalno tijelo za kibernetičkosigurnosnu certifikaciju. O takvom povlačenju obavješćuje i ENISA-u kako bi se olakšalo obavljanje njezine zadaće na temelju članka 50. Uredbe (EU) 2019/881. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju obavješćuje druga relevantna tijela za nadzor tržišta.

3. Nositelj EUCC certifikata može zatražiti povlačenje certifikata.

POGLAVLJE III.

CERTIFIKACIJA PROFILA ZAŠTITE

ODJELJAK I.

Evaluacija: specifične norme i zahtjevi

Članak 15.

Evaluacijski kriteriji i metode

1. Profil zaštite evaluira se minimalno na temelju:

(a) primjenjivih elemenata normi iz članka 3.;

(b) razine rizika povezane s namjenom predmetnih IKT proizvoda u skladu s člankom 52. Uredbe (EU) 2019/881 i njihovim sigurnosnim funkcijama kojima se podupiru sigurnosni ciljevi iz članka 51. te uredbe; i

(c) primjenjivih specifikacija najsuvremenijih tehnika navedenih u Prilogu I. Profil zaštite iz tehničke domene certificira se na temelju zahtjeva utvrđenih u toj tehničkoj domeni.

2. U iznimnim i propisno opravdanim slučajevima tijelo za ocjenjivanje sukladnosti može certificirati profil zaštite bez primjene relevantnih specifikacija najsuvremenijih tehnika. U takvim slučajevima o tome šalje obavijest nadležnom nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju s obrazloženjem planirane certifikacije bez primjene specifikacija najsuvremenijih tehnika i s predloženom evaluacijskom metodologijom. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ocjenjuje to obrazloženje i, ako je opravdano, odobrava neprimjenu relevantnih specifikacija najsuvremenijih tehnika te, prema potrebi, odobrava ili mijenja evaluacijsku metodologiju koju treba primjenjivati tijelo za ocjenjivanje sukladnosti. Do donošenja odluke nacionalnog tijela za kibernetičkosigurnosnu certifikaciju tijelo za ocjenjivanje sukladnosti ne smije izdati nikakav certifikat za taj profil zaštite. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju o odobrenoj neprimjeni relevantnih specifikacija najsuvremenijih tehnika bez nepotrebne odgode obavješćuje Europsku skupinu za kibernetičkosigurnosnu certifikaciju, koja može izdati mišljenje. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju mora koliko je god moguće uzeti u obzir mišljenje Europske skupine za kibernetičkosigurnosnu certifikaciju.

ODJELJAK II.

IZDAVANJE, OBNAVLJANJE I POVLAČENJE EUCC CERTIFIKATA ZA PROFILE ZAŠTITE

Članak 16.

Informacije potrebne za certifikaciju profila zaštite

Podnositelj zahtjeva za certifikaciju profila zaštite certifikacijskom tijelu i ITSEF-u dostavlja ili na drugi način stavlja na raspolaganje sve informacije potrebne za certifikacijske aktivnosti. Članak 8. stavci 2., 3., 4. i 7. primjenjuju se *mutatis mutandis*.

Članak 17.

Izdavanje EUCC certifikata za profile zaštite

1. Podnositelji zahtjeva za certifikaciju certifikacijskom tijelu i ITSEF-u dostavljaju sve potrebne informacije koje moraju biti potpune i točne.

2. Članci 9. i 10. primjenjuju se *mutatis mutandis*.

3. ITSEF evaluira je li profil zaštite potpun, dosljedan, tehnički prihvatljiv i djelotvoran za predviđenu uporabu i sigurnosne ciljeve kategorije IKT proizvoda obuhvaćene tim profilom zaštite.

4. Profil zaštite smije certificirati isključivo:

(a) nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ili drugo javno tijelo akreditirano kao certifikacijsko tijelo; ili

(b) certifikacijsko tijelo, nakon prethodnog odobrenja nacionalnog tijela za kibernetičkosigurnosnu certifikaciju za svaki pojedinačni profil zaštite.

Članak 18.

Razdoblje valjanosti EUCC certifikata za profile zaštite

1. Certifikacijsko tijelo određuje razdoblje valjanosti za svaki EUCC certifikat.

2. Razdoblje valjanosti može trajati najviše do isteka životnog vijeka tog profila zaštite.

Članak 19.

Revizija EUCC certifikata za profile zaštite

1. Na zahtjev nositelja certifikata ili iz drugih opravdanih razloga certifikacijsko tijelo može odlučiti revidirati EUCC certifikat za određeni profil zaštite. U reviziji se primjenjuju uvjeti iz članka 15. Opseg revizije određuje certifikacijsko tijelo. Ako je to potrebno radi revizije, certifikacijsko tijelo zahtijeva od ITSEF-a da provede ponovnu evaluaciju certificiranog profila zaštite.

2. Na temelju rezultata revizije i, prema potrebi, ponovne evaluacije, certifikacijsko tijelo čini jedno od sljedećega:

(a) potvrđuje EUCC certifikat;

(b) povlači EUCC certifikat u skladu s člankom 20.;

(c) povlači EUCC certifikat u skladu s člankom 20. i izdaje novi EUCC certifikat s jednakim opsegom i produljenim razdobljem valjanosti;

(d) povlači EUCC certifikat u skladu s člankom 20. i izdaje novi EUCC certifikat s drukčijim opsegom.

Članak 20.

Povlačenje EUCC certifikata za profil zaštite

1. Ne dovodeći u pitanje članak 58. stavak 8. točku (e) Uredbe (EU) 2019/881, EUCC certifikat za određeni profil zaštite povlači certifikacijsko tijelo koje je taj certifikat izdalo. Članak 14. primjenjuje se *mutatis mutandis*.

2. Certifikat za profil zaštite izdan u skladu s člankom 17. stavkom 4. točkom (b) povlači nacionalno tijelo za kibernetičkosigurnosnu certifikaciju koje je taj certifikat odobrilo.

POGLAVLJE IV.

TIJELA ZA OCJENJIVANJE SUKLADNOSTI

Članak 21.

Dodatni ili posebni zahtjevi za certifikacijsko tijelo

1. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ovlašćuje certifikacijsko tijelo za izdavanje EUCC certifikata s visokom jamstvenom razinom ako to tijelo, uz to što ispunjava zahtjeve za akreditaciju tijela za ocjenjivanje sukladnosti iz članka 60. stavka 1. i Priloga Uredbi (EU) 2019/881, dokaže:

(a) da posjeduje stručnost i kompetencije potrebne za donošenje odluke o certifikaciji na visokoj jamstvenoj razini;

(b) da certifikacijske aktivnosti obavlja u suradnji s ITSEF-om ovlaštenim u skladu s člankom 22.; i

(c) da ima potrebne kompetencije i, uz zahtjeve iz članka 43., primjenjuje odgovarajuće tehničke i operativne mjere za djelotvornu zaštitu povjerljivih i osjetljivih informacija na visokoj jamstvenoj razini.

2. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ocjenjuje ispunjava li certifikacijsko tijelo sve zahtjeve iz stavka 1. To ocjenjivanje uključuje barem strukturirane intervjue i reviziju najmanje jedne probne certifikacije koju je certifikacijsko tijelo provelo u skladu s ovom Uredbom.

Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju u ocjenjivanju može iskoristiti postojeće odgovarajuće dokaze iz prethodne autorizacije ili sličnih aktivnosti dodijeljene na temelju:

(a) ove Uredbe;

(b) drugog europskog programa kibernetičkosigurnosne certifikacije donesenog na temelju članka 49. Uredbe (EU) 2019/881;

(c) nacionalnog programa iz članka 49. ove Uredbe.

3. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju izrađuje izvješće o autorizaciji koje podliježe istorazinskom ocjenjivanju u skladu s člankom 59. stavkom 3. točkom (d) Uredbe (EU) 2019/881.

4. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju određuje kategorije IKT proizvoda i profile zaštite na koje se autorizacija primjenjuje. Razdoblje valjanosti autorizacije ne smije biti dulje od razdoblja valjanosti akreditacije. Autorizacija se može obnoviti na zahtjev pod uvjetom da certifikacijsko tijelo i dalje ispunjava zahtjeve iz ovog članka. Za obnovu autorizacije nisu potrebne probne evaluacije.

5. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju povlači autorizaciju certifikacijskog tijela ako ono više ne ispunjava uvjete iz ovog članka. Nakon povlačenja autorizacije certifikacijsko tijelo odmah se prestaje predstavljati kao autorizirano certifikacijsko tijelo.

Članak 22.

Dodatni ili posebni zahtjevi za ITSEF

1. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ovlašćuje ITSEF za evaluaciju IKT proizvoda koji podliježu certifikaciji za visoku jamstvenu razinu ako ITSEF, uz to što ispunjava zahtjeve iz članka 60. stavka 1. i Priloga Uredbi (EU) 2019/881 u pogledu akreditacije tijela za ocjenjivanje sukladnosti, dokaže da ispunjava sve sljedeće uvjete:

(a) posjeduje potrebnu stručnost za obavljanje evaluacijskih aktivnosti radi utvrđivanja otpornosti na najsuvremenije kibernetičke napade koje izvode subjekti znatnih vještina i resursa;

(b) za tehničke domene i profile zaštite koji su dio IKT procesa za te IKT proizvode, posjeduje:

1. stručnost za obavljanje posebnih evaluacijskih aktivnosti potrebnih da bi se metodički utvrdila otpornost predmeta evaluacije u njegovu operativnom okruženju s obzirom na potencijal za napade „umjerenog” ili „visokog” intenziteta kako su utvrđeni u normama iz članka 3., pod pretpostavkom da su napadači umješni;

2. tehničke kompetencije kako su opisane u specifikacijama najsuvremenijih tehnika navedenih u Prilogu I.

(c) da ima potrebne kompetencije i, uz zahtjeve iz članka 43., primjenjuje odgovarajuće tehničke i operativne mjere za djelotvornu zaštitu povjerljivih i osjetljivih informacija na visokoj jamstvenoj razini.

2. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ocjenjuje ispunjava li ITSEF sve zahtjeve iz stavka 1. To ocjenjivanje uključuje barem strukturirane intervjue i reviziju najmanje jedne probne evaluacije koju je ITSEF proveo u skladu s ovom Uredbom.

3. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju u ocjenjivanju može iskoristiti postojeće odgovarajuće dokaze iz prethodne autorizacije ili sličnih aktivnosti dodijeljene na temelju:

(a) ove Uredbe;

(b) drugog europskog programa kibernetičkosigurnosne certifikacije donesenog na temelju članka 49. Uredbe (EU) 2019/881;

(c) nacionalnog programa iz članka 49. ove Uredbe.

4. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju izrađuje izvješće o autorizaciji koje podliježe istorazinskom ocjenjivanju u skladu s člankom 59. stavkom 3. točkom (d) Uredbe (EU) 2019/881.

5. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju određuje kategorije IKT proizvoda i profile zaštite na koje se autorizacija primjenjuje. Razdoblje valjanosti autorizacije ne smije biti dulje od razdoblja valjanosti akreditacije. Autorizacija se može obnoviti na zahtjev pod uvjetom da ITSEF i dalje ispunjava zahtjeve iz ovog članka. Za obnovu autorizacije ne bi trebalo zahtijevati probne evaluacije.

6. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju povlači autorizaciju ITSEF-a ako on više ne ispunjava uvjete iz ovog članka. Nakon povlačenja autorizacije ITSEF se odmah prestaje predstavljati kao autorizirani ITSEF.

Članak 23.

Prijavljivanje tijela za ovjeravanje

1. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju Komisiji prijavljuje certifikacijska tijela na svojem državnom području koja su na temelju akreditacije nadležna za certifikaciju na znatnoj jamstvenoj razini.

2. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju Komisiji prijavljuje certifikacijska tijela na svojem državnom području koja su na temelju akreditacije i odluke o autorizaciji nadležna za certifikaciju na visokoj jamstvenoj razini.

3. Pri prijavljivanju certifikacijskih tijela Komisiji nacionalno tijelo za kibernetičkosigurnosnu certifikaciju dostavlja barem sljedeće informacije:

(a) jamstvene razine za koje certifikacijsko tijelo može izdavati EUCC certifikate;

(b) sljedeće informacije povezane s akreditacijom:

1. datum akreditacije;

2. ime i adresu tijela za certifikaciju;

3. državu registracije tijela za certifikaciju;

4. referentni broj akreditacije;

5. opseg i razdoblje valjanosti akreditacije;

6. adresu, lokaciju i poveznicu na internetske stranice nacionalnog akreditacijskog tijela; i

(c) sljedeće informacije povezane s autorizacijom za visoku razinu:

1. datum autorizacije;

2. referentni broj autorizacije;

3. razdoblje valjanosti autorizacije;

4. opseg autorizacije uključujući najvišu razinu AVA_VAN i, ako je primjenjivo, obuhvaćenu tehničku domenu.

4. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ENISA-i šalje primjerak obavijesti iz stavaka 1. i 2. radi objave točnih informacija o prihvatljivosti certifikacijskih tijela na internetskim stranicama o kibernetičkosigurnosnoj certifikaciji.

5. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju bez nepotrebne odgode provjerava sve informacije o promjeni statusa akreditacije koje dostavi nacionalno akreditacijsko tijelo. Ako je akreditacija ili autorizacija povučena, nacionalno tijelo za kibernetičkosigurnosnu certifikaciju o tome obavješćuje Komisiju i može Komisiji podnijeti zahtjev u skladu s člankom 61. stavkom 4. Uredbe (EU) 2019/881.

Članak 24.

Obavješćivanje o ITSEF-u

Obveze nacionalnih tijela za kibernetičkosigurnosnu certifikaciju u pogledu obavješćivanja iz članka 23. primjenjuju se i na ITSEF. Obavijest mora sadržavati adresu ITSEF-a, valjanu akreditaciju i, ako je primjenjivo, valjanu autorizaciju tog ITSEF-a.

POGLAVLJE V.

PRAĆENJE, NESUKLADNOST I NEPOŠTOVANJE OBVEZA

ODJELJAK I.

Praćenje poštovanja obveza

Članak 25.

Aktivnosti praćenja koje provodi nacionalno tijelo za kibernetičkosigurnosnu certifikaciju

1. Ne dovodeći u pitanje članak 58. stavak 7. Uredbe (EU) 2019/881 nacionalno tijelo za kibernetičkosigurnosnu certifikaciju prati:

(a) poštuju li certifikacijsko tijelo i ITSEF svoje obveze iz ove Uredbe i Uredbe (EU) 2019/881;

(b) poštuju li nositelji EUCC certifikata svoje obveze iz ove Uredbe i Uredbe (EU) 2019/881;

(c) jesu li certificirani IKT proizvodi sukladni sa zahtjevima EUCC-a;

(d) je li jamstvo navedeno u EUCC certifikatu primjereno za prijetnje koje se stalno mijenjaju.

2. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju svoje aktivnosti praćenja obavlja prije svega na temelju:

(a) informacija koje dostavljaju certifikacijska tijela, nacionalna akreditacijska tijela i relevantna tijela za nadzor tržišta;

(b) informacija dobivenih iz revizija i istraga koje je provelo ono samo ili koje su provela druga tijela;

(c) uzorkovanja provedenog u skladu sa stavkom 3.;

(d) zaprimljenih pritužbi.

3. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju u suradnji s drugim tijelima za nadzor tržišta godišnje uzorkuje najmanje 4 % EUCC certifikata kako je utvrđeno procjenom rizika. Tom tijelu u praćenju sukladnosti i poštovanja obveza na zahtjev i u ime nadležnog nacionalnog tijela za kibernetičkosigurnosnu certifikaciju pomažu certifikacijska tijela i, ako je to potrebno, ITSEF.

4. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju uzorak certificiranih IKT proizvoda koje treba provjeriti odabire na temelju objektivnih kriterija među kojima su:

(a) kategorija proizvoda;

(b) jamstvene razine proizvoda;

(c) nositelj certifikata;

(d) certifikacijsko tijelo i, ako je primjenjivo, podugovoreni ITSEF;

(e) sve druge informacije s kojima je to tijelo upoznato.

5. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju obavješćuje nositelje EUCC certifikata o odabranim IKT proizvodima i kriterijima odabira.

6. Certifikacijsko tijelo koje je certificiralo uzorkovani IKT proizvod na zahtjev nacionalnog tijela za kibernetičkosigurnosnu certifikaciju uz pomoć tog ITSEF-a provodi dodatnu reviziju u skladu s postupkom iz odjeljka IV.2. Priloga IV. i o rezultatima obavješćuje nacionalno tijelo za kibernetičkosigurnosnu certifikaciju.

7. Ako nacionalno tijelo za kibernetičkosigurnosnu certifikaciju ima dovoljno razloga smatrati da certificirani IKT proizvod više nije sukladan s ovom Uredbom ili Uredbom (EU) 2019/881, ono može provoditi istrage ili iskoristiti bilo koju drugu ovlast praćenja iz članka 58. stavku 8. Uredbe (EU) 2019/881.

8. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju obavješćuje certifikacijsko tijelo i ITSEF o istragama koje su u tijeku u vezi s odabranim IKT proizvodima.

9. Ako nacionalno tijelo za kibernetičkosigurnosnu certifikaciju utvrdi da se istraga koja je u tijeku odnosi na IKT proizvode koje su certificirala certifikacijska tijela s poslovnim nastanom u drugim državama članicama, o tome obavješćuje nacionalna tijela za kibernetičkosigurnosnu certifikaciju relevantnih država članica kako bi, prema potrebi, surađivala u istragama. To nacionalno tijelo za kibernetičkosigurnosnu certifikaciju također bez nepotrebne odgode o prekograničnim istragama i njihovim rezultatima obavješćuje Europsku skupinu za kibernetičkosigurnosnu certifikaciju.

Članak 26.

Aktivnosti praćenja koje provodi certifikacijsko tijelo

1. Certifikacijsko tijelo prati:

(a) poštuju li nositelji certifikata svoje obveze iz ove Uredbe i Uredbe (EU) 2019/881 u pogledu EUCC certifikata koji je izdalo to certifikacijsko tijelo;

(b) jesu li IKT proizvodi koje je certificiralo sukladni sa sigurnosnim zahtjevima koji se odnose na njih

(c) jamstvo navedeno u certificiranim profilima zaštite.

2. Certifikacijsko tijelo svoje aktivnosti praćenja provodi na temelju:

(a) informacija koje podnositelj zahtjeva za certifikaciju dostavlja na temelju obveza iz članka 9. stavka 2.;

(b) informacija koje proizlaze iz aktivnosti drugih relevantnih tijela za nadzor tržišta;

(c) zaprimljenih pritužbi;

(d) informacija o ranjivostima koje bi mogle utjecati na IKT proizvode koje je to tijelo certificiralo.

3. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju može sastaviti pravila za redoviti dijalog između certifikacijskih tijela i nositelja EUCC certifikata radi provjere i izvješćivanja o sukladnosti i poštovanju obveza preuzetih na temelju članka 9. stavka 2., ne dovodeći u pitanje aktivnosti povezane s drugim relevantnim tijelima za nadzor tržišta.

Članak 27.

Aktivnosti praćenja koje provodi nositelj certifikata

1. Nositelj EUCC certifikata obavlja sljedeće zadaće radi praćenja sukladnosti certificiranog IKT proizvoda sa sigurnosnim zahtjevima koji se na njega primjenjuju:

(a) prati informacije o ranjivostima povezanima s certificiranim IKT proizvodom, uključujući poznate ovisnosti, vlastitim sredstvima, ali i uzimajući u obzir:

1. objavu ili podnesak korisnika ili istraživača u području sigurnosti o ranjivostima primljenima u skladu s člankom 55. stavkom 1. točkom (c) Uredbe (EU) 2019/881;

2. podnesak iz bilo kojeg drugog izvora;

(b) prati jamstvo navedeno u EUCC certifikatu.

2. Nositelj EUCC certifikata surađuje s certifikacijskim tijelom, ITSEF-om i, prema potrebi, nacionalnim tijelom za kibernetičkosigurnosnu certifikaciju kako bi im pomogao u aktivnostima praćenja.

ODJELJAK II.

SUKLADNOST I POŠTOVANJE OBVEZA

Članak 28.

Posljedice nesukladnosti certificiranog IKT proizvoda ili profila zaštite

1. Ako certificirani IKT proizvod ili profil zaštite nije sukladan sa zahtjevima iz ove Uredbe i Uredbe (EU) 2019/881, certifikacijsko tijelo obavješćuje nositelja EUCC certifikata o utvrđenoj nesukladnosti i zahtijeva korektivne mjere.

2. Ako bi slučaj nesukladnosti s odredbama ove Uredbe mogao utjecati na poštovanje odredbi iz drugih relevantnih propisa Unije u kojima je propisana mogućnost da se pretpostavka sukladnosti sa zahtjevima tog pravnog akta dokaže EUCC certifikatom, certifikacijsko tijelo o tome bez odgode obavješćuje nacionalno tijelo za kibernetičkosigurnosnu certifikaciju. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju odmah o utvrđenom slučaju nesukladnosti obavješćuje tijelo za nadzor tržišta odgovorno za takve druge relevantne zakonodavne propise Unije.

3. Po primitku informacija iz stavka 1. nositelj EUCC certifikata u roku koji odredi certifikacijsko tijelo, a koji ne smije biti dulji od 30 dana, certifikacijskom tijelu predlaže korektivne mjere potrebne za uklanjanje nesukladnosti.

4. Certifikacijsko tijelo može u hitnim slučajevima, ili u slučajevima kad nositelj EUCC certifikata ne surađuje propisno s certifikacijskim tijelom, bez nepotrebne odgode suspendirati EUCC certifikat u skladu s člankom 30.

5. Certifikacijsko tijelo provodi reviziju u skladu s člancima 13. i 19. kako bi procijenilo utjecaj korektivnih mjera na uklanjanje nesukladnosti.

6. Ako nositelj EUCC certifikata ne predloži odgovarajuće korektivne mjere u roku iz stavka 3., certifikat se suspendira u skladu s člankom 30. ili povlači u skladu s člankom 14. ili 20.

7. Ovaj se članak ne primjenjuje na slučajeve ranjivosti koji utječu na certificirani IKT proizvod, s kojima se postupa u skladu s poglavljem VI.

Članak 29.

Posljedice ako obveze ne poštuje nositelj certifikata

1. Ako certifikacijsko tijelo utvrdi da:

(a) nositelj EUCC certifikata ili podnositelj zahtjeva za certifikaciju ne poštuje svoje obveze iz članka 9. stavka 2., članka 17. stavka 2. te članaka 27. i 41.; ili

(b) nositelj EUCC certifikata ne poštuje članak 56. stavak 8. Uredbe (EU) 2019/881 ili poglavljem VI. ove Uredbe;

utvrđuje rok od najviše 30 dana u kojem je nositelj EUCC certifikata dužan poduzeti korektivne mjere.

2. Ako nositelj EUCC certifikata ne predloži odgovarajuće korektivne mjere u roku iz stavka 1., certifikat se suspendira u skladu s člankom 30. ili povlači u skladu s člancima 14. i 20.

3. Ako nositelj EUCC certifikata trajno ili opetovano krši obveze iz stavka 1., to dovodi do povlačenja EUCC certifikata u skladu s člankom 14. ili 20.

4. Certifikacijsko tijelo o nalazima iz stavka 1. obavješćuje nacionalno tijelo za kibernetičkosigurnosnu certifikaciju. Ako slučaj nepoštovanja utječe na poštovanje drugih relevantnih propisa Unije, nacionalno tijelo za kibernetičkosigurnosnu certifikaciju o utvrđenom slučaju nepoštovanja odmah obavješćuje tijelo za nadzor tržišta odgovorno za te druge relevantne propise Unije.

Članak 30.

Suspenzija EUCC certifikata

1. U slučaju suspenzije EUCC certifikata na temelju ove Uredbe certifikacijsko tijelo suspendira predmetni EUCC certifikat na razdoblje primjereno okolnostima koje su dovele do suspenzije, a koje ne smije biti dulje od 42 dana. Razdoblje suspenzije počinje teći sljedećeg dana od dana odluke certifikacijskog tijela. Suspenzija ne utječe na valjanost certifikata.

2. Certifikacijsko tijelo o suspenziji bez nepotrebne odgode obavješćuje nositelja certifikata i nacionalno tijelo za kibernetičkosigurnosnu certifikaciju te navodi razloge za suspenziju, zatražene mjere koje treba poduzeti i razdoblje suspenzije.

3. Nositelji certifikata obavješćuju kupce predmetnih IKT proizvoda o suspenziji i razlozima za suspenziju koje je navelo certifikacijsko tijelo, izuzev onih dijelova razloga čije bi dijeljenje predstavljalo sigurnosni rizik ili koji sadržavaju osjetljive informacije. Nositelj certifikata te informacije također javno objavljuje.

4. Ako je u drugim relevantnim propisima Unije predviđena pretpostavka sukladnosti na temelju certifikata izdanih u skladu s odredbama ove Uredbe, nacionalno tijelo za kibernetičkosigurnosnu certifikaciju o suspenziji obavješćuje tijelo za nadzor tržišta odgovorno za to drugo relevantno zakonodavstvo Unije.

5. ENISA se obavješćuje o suspenziji certifikata u skladu s člankom 42. stavkom 3.

6. U opravdanim slučajevima nacionalno tijelo za kibernetičkosigurnosnu certifikaciju može odobriti produljenje razdoblja suspenzije EUCC certifikata. Ukupno razdoblje suspenzije ne može biti dulje od jedne godine.

Članak 31.

Posljedice ako obveze ne poštuje tijelo za ocjenjivanje sukladnosti

1. Ako certifikacijsko tijelo ne poštuje svoje obveze ili ako ih ne poštuje relevantno certifikacijsko tijelo u slučaju da se utvrdi nesukladnost ITSEF-a, nacionalno tijelo za kibernetičkosigurnosnu certifikaciju bez nepotrebne odgode:

(a) utvrđuje, uz potporu predmetnog ITSEF-a, EUCC certifikate na koje bi to moglo utjecati;

(b) kako bi se olakšalo to utvrđivanje, prema potrebi zahtijeva da ITSEF koji je izvršio evaluaciju ili bilo koji drugi akreditirani te, ako je primjenjivo, autorizirani ITSEF koji je za to tehnički opremljeniji provede evaluacijske aktivnosti na jednom ili više IKT proizvoda ili profila zaštite;

(c) analizira posljedice nepoštovanja obveza;

(d) o tome obavješćuje nositelja EUCC certifikata na kojeg utječe nepoštovanje obveza.

2. Na temelju mjera iz stavka 1. certifikacijsko tijelo za svaki pogođeni EUCC certifikat donosi jednu od sljedećih odluka:

(a) ne mijenja EUCC certifikat;

(b) povlači EUCC certifikat u skladu s člankom 14. ili 20. i, prema potrebi, izdaje novi EUCC certifikat.

3. Na temelju mjera iz stavka 1. nacionalno tijelo za kibernetičkosigurnosnu certifikaciju:

(a) prema potrebi, izvješćuje nacionalno akreditacijsko tijelo o tome da certifikacijsko tijelo ili povezani ITSEF ne poštuje obveze;

(b) ako je primjenjivo, procjenjuje mogući učinak na autorizaciju.

POGLAVLJE VI.

UPRAVLJANJE RANJIVOSTIMA I OBAVJEŠĆIVANJE O NJIMA

Članak 32.

Opseg upravljanja ranjivostima

Ovo se poglavlje primjenjuje na IKT proizvode za koje je izdan EUCC certifikat.

ODJELJAK I.

UPRAVLJANJE RANJIVOSTIMA

Članak 33.

Postupci upravljanja ranjivostima

1. Nositelj EUCC certifikata uvodi i provodi sve potrebne postupke upravljanja ranjivostima u skladu s pravilima utvrđenima u ovom odjeljku i, prema potrebi, uz dopunu postupcima utvrđenima u normi EN ISO/IEC 30111.

2. Nositelj EUCC certifikata održava i objavljuje odgovarajuće načine primanja informacija o ranjivostima povezanima sa svojim proizvodima iz vanjskih izvora, među ostalim od korisnika, certifikacijskih tijela i istraživača u području sigurnosti.

3. Ako nositelj EUCC certifikata otkrije ili primi informacije o mogućoj ranjivosti koja utječe na certificirani IKT proizvod, dužan je to evidentirati i provesti analizu utjecaja ranjivosti.

4. Ako moguća ranjivost utječe na složeni proizvod, nositelj EUCC certifikata o njoj obavješćuje nositelja ovisnih EUCC certifikata.

5. Na razuman zahtjev certifikacijskog tijela koje je izdalo certifikat nositelj EUCC certifikata tom certifikacijskom tijelu dostavlja sve relevantne informacije o mogućim ranjivostima.

Članak 34.

Analiza utjecaja ranjivosti

1. Analiza utjecaja ranjivosti odnosi se na predmet evaluacije i izjave o jamstvu sadržane u certifikatu. Analiza utjecaja ranjivosti provodi se u roku koji je primjeren s obzirom na iskoristivost i kritičnost moguće ranjivosti certificiranog IKT proizvoda.

2. Ako je primjenjivo, potencijal za napad izračunava se primjenom relevantne metodologije navedene u normama iz članka 3. i relevantnih specifikacija najsuvremenijih tehnika iz Priloga I. kako bi se utvrdila iskoristivost ranjivosti. Pritom se mora uzeti u obzir razina AVA_VAN tog EUCC certifikata.

Članak 35.

Izvješće o analizi utjecaja ranjivosti

1. Nositelj izrađuje izvješće o analizi utjecaja ranjivosti ako ta analiza pokaže da ranjivost vjerojatno utječe na sukladnost IKT proizvoda s njegovim certifikatom.

2. Izvješće o analizi utjecaja ranjivosti sadržava procjenu sljedećih elemenata:

(a) utjecaja ranjivosti na certificirani IKT proizvod;

(b) mogućih rizika povezanih s blizinom napada ili raspoloživošću napada;

(c) mogućnosti da se ranjivost otkloni;

(d) ako se ranjivost može otkloniti, moguće načine da se to učini.

3. Izvješće o analizi utjecaja ranjivosti sadržava, ako je primjenjivo, detaljne podatke o mogućim načinima iskorištavanja ranjivosti. S informacijama koje se odnose na moguće načine iskorištavanja ranjivosti postupa se u skladu s odgovarajućim sigurnosnim mjerama kako bi se zaštitila njihova povjerljivost i, prema potrebi, zajamčila njihova ograničena distribucija.

4. Nositelj EUCC certifikata bez nepotrebne odgode dostavlja izvješće o analizi utjecaja ranjivosti certifikacijskom tijelu ili nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju u skladu s člankom 56. stavkom 8. Uredbe (EU) 2019/881.

5. Ako se u izvješću o analizi utjecaja ranjivosti utvrdi da ranjivost nije rezidualna u smislu normi iz članka 3. i da se može otkloniti, primjenjuje se članak 36.

6. Ako se u izvješću o analizi utjecaja ranjivosti utvrdi da ranjivost nije rezidualna i da se ne može otkloniti, EUCC certifikat povlači se u skladu s člankom 14.

7. Nositelj EUCC certifikata prati sve rezidualne ranjivosti kako bi osigurao da se one ne mogu iskoristiti u slučaju promjena u radnom okruženju.

Članak 36.

Otklanjanje ranjivosti

Nositelj EUCC certifikata certifikacijskom tijelu podnosi prijedlog odgovarajućih korektivnih mjera. Certifikacijsko tijelo revidira certifikat u skladu s člankom 13. Opseg revizije određuje se prema predloženom otklanjanju ranjivosti.

ODJELJAK II.

OBAVJEŠĆIVANJE O RANJIVOSTIMA

Članak 37.

Informacije koje se dostavljaju nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju

1. Informacije koje certifikacijsko tijelo dostavlja nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju moraju sadržavati sve elemente koji su nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju potrebni za razumijevanje utjecaja ranjivosti, izmjene koje je potrebno napraviti na IKT proizvodu i, ako su dostupne, sve informacije kojima certifikacijsko tijelo raspolaže o širim posljedicama ranjivosti na druge certificirane IKT proizvode.

2. Informacije dostavljene u skladu sa stavkom 1. ne smiju sadržavati detalje o tome kako se ranjivost može iskoristiti. Ovom se odredbom ne dovode u pitanje istražne ovlasti nacionalnog tijela za kibernetičkosigurnosnu certifikaciju.

Članak 38.

Suradnja s drugim nacionalnim tijelima za kibernetičkosigurnosnu certifikaciju

1. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju dijeli relevantne informacije primljene u skladu s člankom 37. s drugim nacionalnim tijelima za kibernetičkosigurnosnu certifikaciju i ENISA-om.

2. Druga nacionalna tijela za kibernetičkosigurnosnu certifikaciju mogu odlučiti da će dodatno analizirati ranjivost ili da će, nakon što o tome obavijeste nositelja EUCC certifikata, od relevantnih certifikacijskih tijela zatražiti da procijene može li ranjivost utjecati na druge certificirane IKT proizvode.

Članak 39.

Objava utvrđene ranjivosti

Nakon povlačenja certifikata nositelj EUCC certifikata objavljuje i evidentira sve javno poznate i otklonjene ranjivosti u IKT proizvodu u europskoj bazi podataka o ranjivostima uspostavljenoj u skladu s člankom 12. Direktive (EU) 2022/2555

Europskog parlamenta i Vijeća ([5]) ili u drugim internetskim repozitorijima iz članka 55. stavka 1. točke (d) Uredbe (EU) 2019/881.

POGLAVLJE VII.

ČUVANJE, OTKRIVANJE I ZAŠTITA INFORMACIJA

Članak 40.

Čuvanje evidencije certifikacijskih tijela i ITSEF-a

1. ITSEF i certifikacijska tijela vode sustav evidencije koji sadržava sve dokumente izrađene u vezi sa svakom evaluacijom i certifikacijom koju provedu.

2. Certifikacijska tijela i ITSEF dužna su evidenciju pohranjivati na siguran način te je čuvati u razdoblju nužnom za potrebe ove Uredbe i najmanje pet godina nakon povlačenja relevantnog EUCC certifikata. Ako je certifikacijsko tijelo izdalo novi EUCC certifikat u skladu s člankom 13. stavkom 2. točkom (c), ono uz taj novi certifikat mora čuvati dokumentaciju povučenog EUCC certifikata i to jednako dugo koliko i dokumentaciju novog certifikata.

Članak 41.

Informacije koje na raspolaganje stavlja nositelj certifikata

1. Informacije iz članka 55. Uredbe (EU) 2019/881 moraju biti dostupne na jeziku koji je korisnicima lako razumljiv.

2. Nositelj EUCC certifikata dužan je na siguran način te u razdoblju nužnom za potrebe ove Uredbe i najmanje pet godina nakon povlačenja relevantnog EUCC certifikata čuvati:

(a) evidenciju informacija koje su u postupku certifikacije dostavljene certifikacijskom tijelu i ITSEF-u;

(b) ogledni primjerak certificiranog IKT proizvoda.

3. Ako je certifikacijsko tijelo izdalo novi EUCC certifikat u skladu s člankom 13. stavkom 2. točkom (c), nositelj uz taj novi certifikat mora čuvati dokumentaciju povučenog EUCC certifikata i to jednako dugo koliko i dokumentaciju novog certifikata.

4. Na zahtjev certifikacijskog tijela ili nacionalnog tijela za kibernetičkosigurnosnu certifikaciju nositelj EUCC certifikata stavlja na raspolaganje evidenciju i kopiju informacija iz stavka 2.

Članak 42.

Informacije koje na raspolaganje stavlja ENISA

1. ENISA na internetskim stranicama iz članka 50. stavka 1. Uredbe (EU) 2019/881 objavljuje sljedeće informacije:

(a) sve EUCC certifikate;

(b) informacije o statusu EUCC certifikata, konkretno o tome je li certifikat na snazi, suspendiran, povučen ili istekao;

(c) izvješća o certifikaciji za svaki EUCC certifikat;

([5]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

(d) popis akreditiranih tijela za ocjenjivanje sukladnosti;

(e) popis autoriziranih tijela za ocjenjivanje sukladnosti;

(f) specifikacije najsuvremenijih tehnika iz Priloga I.;

(g) mišljenja Europske skupine za kibernetičkosigurnosnu certifikaciju iz članka 62. stavka 4. točke (c) Uredbe (EU) 2019/881;

(h) izvješća o istorazinskoj ocjeni izdana u skladu s člankom 47.

2. Informacije iz stavka 1. moraju biti barem na engleskom jeziku.

3. Certifikacijska tijela i, prema potrebi, nacionalna tijela za kibernetičkosigurnosnu certifikaciju bez nepotrebne odgode obavješćuju ENISA-u o svojim odlukama koje utječu na sadržaj ili status EUCC certifikata iz stavka 1. točke (b).

4. ENISA vodi računa o tome da su u informacijama objavljenima u skladu sa stavkom 1. točkama (a), (b) i (c) jasno navedene verzije certificiranog IKT proizvoda na koje se EUCC certifikat odnosi.

Članak 43.

Zaštita informacija

Tijela za ocjenjivanje sukladnosti, nacionalna tijela za kibernetičkosigurnosnu certifikaciju, Europska skupina za kibernetičkosigurnosnu certifikaciju, ENISA, Komisija i sve druge strane dužne su se pobrinuti za sigurnost i zaštitu poslovnih tajni i drugih povjerljivih informacija, uključujući trgovinske tajne, i štititi prava intelektualnog vlasništva pa poduzimaju potrebne i odgovarajuće tehničke i organizacijske mjere.

POGLAVLJE VIII.

SPORAZUMI O UZAJAMNOM PRIZNAVANJU S TREĆIM ZEMLJAMA

Članak 44.

Uvjeti

1. Treće zemlje koje žele certificirati svoje proizvode u skladu s ovom Uredbom i koje žele da takva certifikacija bude priznata u Uniji s Unijom sklapaju sporazum o uzajamnom priznavanju.

2. Sporazum o uzajamnom priznavanju obuhvaća primjenjive jamstvene razine za certificirane IKT proizvode i, prema potrebi, profile zaštite.

3. Sporazumi o uzajamnom priznavanju iz stavka 1. mogu se sklapati samo s trećim zemljama koje ispunjavaju sljedeće uvjete:

(a) imaju tijelo:

1. koje je javno tijelo, neovisno o subjektima koje nadzire i prati u smislu organizacijske i pravne strukture, financiranja i donošenja odluka;

2. koje ima odgovarajuće ovlasti za praćenje i nadzor u svrhu provedbe istraga i ovlašteno je poduzeti odgovarajuće korektivne mjere radi postizanja sukladnosti;

3. koje ima učinkovit, proporcionalan i odvraćajući sustav sankcija kako bi se zajamčila sukladnost;

4. koje je prihvatilo suradnju s Europskom skupinom za kibernetičkosigurnosnu certifikaciju i ENISA-om radi razmjene primjera dobre prakse i relevantnih kretanja u području kibernetičkosigurnosne certifikacije te raditi na ujednačenom tumačenju evaluacijskih kriterija i metoda koji su trenutačno u primjeni, među ostalim korištenjem usklađene dokumentacije koja je jednakovrijedna specifikacijama najsuvremenijih tehnika iz Priloga I.;

(b) imaju neovisno akreditacijsko tijelo koje provodi akreditaciju uz primjenu normi jednakovrijednih onima iz Uredbe (EZ) br. 765/2008;

(c) obvezale su se da će se procesi i postupci evaluacije i certifikacije provoditi na propisno profesionalan način, vodeći računa o poštovanju međunarodnih normi iz ove Uredbe, a posebno članka 3.;

(d) imaju kapacitet za izvješćivanje o prethodno neotkrivenim ranjivostima i uspostavljen prikladan postupak za upravljanje ranjivostima i obavješćivanje o njima;

(e) imaju uspostavljene postupke koji omogućuju djelotvorno podnošenje i rješavanje pritužbi i daju djelotvoran pravni lijek podnositelju pritužbe;

(f) uspostavile su mehanizam za suradnju s drugim tijelima Unije i država članica relevantnima za kibernetičkosigurnosnu certifikaciju na temelju ove Uredbe, među ostalim u obliku razmjene informacija o mogućoj nesukladnosti certifikata, praćenja relevantnih kretanja u području certifikacije i zauzimanja zajedničkog pristupa održavanju i reviziji certifikacije.

4. Uz uvjete iz stavka 3., sporazum o uzajamnom priznavanju iz stavka 1. koji se odnosi na visoku jamstvenu razinu s trećim se zemljama može sklopiti samo ako su ispunjeni i sljedeći uvjeti:

(a) treća zemlja ima neovisno i javno tijelo za kibernetičkosigurnosnu certifikaciju koje provodi ili delegira evaluacijske aktivnosti potrebne za certifikaciju na visokoj jamstvenoj razini koje su jednakovrijedne zahtjevima i postupcima utvrđenima za nacionalna tijela za kibernetičku sigurnost u ovoj Uredbi i Uredbi (EU) 2019/881;

(b) sporazumom o uzajamnom priznavanju uspostavlja se zajednički mehanizam jednakovrijedan istorazinskoj ocjeni za EUCC certifikaciju kako bi se potaknula razmjena praksi i zajednički rješavali problemi u području evaluacije i certifikacije.

POGLAVLJE IX.

ISTORAZINSKO OCJENJIVANJE CERTIFIKACIJSKIH TIJELA

Članak 45.

Postupak istorazinskog ocjenjivanja

1. Certifikacijsko tijelo koje izdaje EUCC certifikate na visokoj jamstvenoj razini redovito se, a najmanje jednom svakih pet godina, podvrgava istorazinskom ocjenjivanju. Vrste istorazinskog ocjenjivanja navedene su u Prilogu VI.

2. Europska skupina za kibernetičkosigurnosnu certifikaciju sastavlja i ažurira raspored istorazinskog ocjenjivanja kako bi se poštovala ta učestalost. Osim u opravdanim slučajevima, istorazinska ocjenjivanja provode se na terenu.

3. Istorazinsko ocjenjivanje može se temeljiti na dokazima iz prethodnih istorazinskih ocjenjivanja ili jednakovrijednih postupaka certifikacijskog tijela koje se istorazinski ocjenjuje ili nacionalnog tijela za kibernetičkosigurnosnu certifikaciju, pod sljedećim uvjetima:

(a) ti rezultati nisu stariji od pet godina;

(b) tim je rezultatima priložen opis postupaka istorazinskog ocjenjivanja koji su uvedeni za taj program ako se odnose na istorazinsko ocjenjivanje provedeno u okviru drugog programa certifikacije;

(c) u izvješću o istorazinskom ocjenjivanju iz članka 47. navodi se koji su postojeći rezultati iskorišteni uz dodatno ocjenjivanje i koji su iskorišteni bez dodatnog ocjenjivanja.

4. Ako istorazinsko ocjenjivanje obuhvaća tehničku domenu, ocjenjuje se i predmetni ITSEF.

5. Certifikacijsko tijelo koje se istorazinski ocjenjuje i, prema potrebi, nacionalno tijelo za kibernetičkosigurnosnu certifikaciju vode računa o tome da tim za istorazinsko ocjenjivanje dobije sve relevantne informacije.

6. Istorazinsko ocjenjivanje provodi tim za istorazinsko ocjenjivanje osnovan u skladu s Prilogom VI.

Članak 46.

Faze istorazinskog ocjenjivanja

1. U pripremnoj fazi članovi tima za istorazinsko ocjenjivanje pregledavaju dokumentaciju certifikacijskog tijela u kojoj se navode njegove politike i postupci, uključujući u vezi s primjenom specifikacija najsuvremenijih tehnika.

2. U fazi terenskog posjeta tim za istorazinsko ocjenjivanje ocjenjuje tehničku kompetentnost tijela i, ako je primjenjivo, kompetentnost ITSEF-a koji je proveo barem jednu evaluaciju IKT proizvoda obuhvaćenu istorazinskim ocjenjivanjem.

3. Trajanje faze terenskog posjeta može se produljiti ili skratiti ovisno o čimbenicima kao što su mogućnost iskorištavanja postojećih dokaza i rezultata istorazinskog ocjenjivanja ili broj ITSEF-a i tehničkih domena za koje certifikacijsko tijelo izdaje certifikate.

4. Ako je primjenjivo, tim za istorazinsko ocjenjivanje određuje tehničku kompetentnost svakog ITSEF-a na temelju posjeta njegovim tehničkim laboratorijima i intervjua evaluatora o tehničkim domenama i povezanim posebnim metodama napada.

5. U fazi izvješćivanja ocjenjivački tim dokumentira svoje nalaze u izvješću o istorazinskom ocjenjivanju, uključujući ocjenu i, prema potrebi, popis uočenih nesukladnosti, od kojih se svaka rangira na ljestvici kritičnosti.

6. Izvješće o istorazinskom ocjenjivanju prvo se mora raspraviti s certifikacijskim tijelom koje se istorazinski ocjenjuje. Nakon te rasprave certifikacijsko tijelo koje se istorazinski ocjenjuje sastavlja popis mjera koje treba poduzeti u vezi s nalazima.

Članak 47.

Izvješće o istorazinskom ocjenjivanju

1. Tim za istorazinsko ocjenjivanje dostavlja nacrt izvješća o istorazinskom ocjenjivanju certifikacijskom tijelu koje se istorazinski ocjenjuje.

2. Certifikacijsko tijelo koje se istorazinski ocjenjuje timu za istorazinsko ocjenjivanje dostavlja primjedbe na nalaz i popis obveza na koje se obvezalo radi uklanjanja nedostataka utvrđenih u nacrtu izvješća o istorazinskom ocjenjivanju.

3. Tim za istorazinsko ocjenjivanje Europskoj skupini za kibernetičkosigurnosnu certifikaciju podnosi završno izvješće o istorazinskom ocjenjivanju koje uključuje primjedbe certifikacijskog tijela koje se istorazinski ocjenjuje i obveze koje je to tijelo preuzelo. Tim za istorazinsko ocjenjivanje također navodi svoje stajalište o primjedbama i o tome jesu li preuzete obveze dovoljne za uklanjanje utvrđenih nedostataka.

4. Ako su u izvješću o istorazinskom ocjenjivanju utvrđene nesukladnosti, Europska skupina za kibernetičkosigurnosnu certifikaciju može odrediti primjereni rok u kojem certifikacijsko tijelo koje se istorazinski ocjenjuje mora te nesukladnosti ukloniti.

5. Europska skupina za kibernetičkosigurnosnu certifikaciju donosi mišljenje o izvješću o istorazinskom ocjenjivanju:

(a) ako u izvješću o istorazinskom ocjenjivanju nisu utvrđene nesukladnosti ili ako je certifikacijsko tijelo koje se istorazinski ocjenjuje nesukladnosti uklonilo na odgovarajući način, Europska skupina za kibernetičkosigurnosnu certifikaciju može izdati pozitivno mišljenje, a svi relevantni dokumenti objavljuju se na ENISA-inim internetskim stranicama o certifikaciji;

(b) ako certifikacijsko tijelo koje se istorazinski ocjenjuje u utvrđenom roku ne ukloni nesukladnosti na odgovarajući način, Europska skupina za kibernetičkosigurnosnu certifikaciju može izdati negativno mišljenje koje se zajedno s izvješćem o istorazinskom ocjenjivanju i svim relevantnim dokumentima objavljuje na ENISA-inim internetskim stranicama o certifikaciji.

6. Prije objave mišljenja iz dokumenata za objavu uklanjaju se sve osjetljive, osobne ili zaštićene informacije.

POGLAVLJE X.

ODRŽAVANJE PROGRAMA

Članak 48.

Održavanje EUCC-a

1. Komisija može od Europske skupine za kibernetičkosigurnosnu certifikaciju zatražiti da donese mišljenje o održavanju EUCC-a i da poduzme potrebne pripremne radnje.

2. Europska skupina za kibernetičkosigurnosnu certifikaciju može donijeti mišljenje kojim podržava specifikacije najsuvremenijih tehnika.

3. ENISA objavljuje specifikacije najsuvremenijih tehnika koje podrži Europska skupina za kibernetičkosigurnosnu certifikaciju.

POGLAVLJE XI.

ZAVRŠNE ODREDBE

Članak 49.

Nacionalni programi obuhvaćeni EUCC-om

1. U skladu s člankom 57. stavkom 1. Uredbe (EU) 2019/881 i ne dovodeći u pitanje članak 57. stavak 3. te uredbe svi nacionalni programi kibernetičkosigurnosne certifikacije i povezani postupci za IKT proizvode i IKT procese koji su obuhvaćeni EUCC-om prestaju proizvoditi učinke 12 mjeseci nakon stupanja na snagu ove Uredbe.

2. Odstupajući od članka 50., certifikacijski postupak može se pokrenuti u okviru nacionalnog programa kibernetičkosigurnosne certifikacije unutar 12 mjeseci od stupanja na snagu ove Uredbe pod uvjetom da ga se završi u roku od 24 mjeseca od stupanja na snagu ove Uredbe.

3. Certifikati izdani u okviru nacionalnih programa kibernetičkosigurnosne certifikacije mogu biti predmet revizije. Novi certifikati koji zamjenjuju revidirane certifikate izdaju se u skladu s ovom Uredbom.

Članak 50.

Stupanje na snagu

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

Primjenjuje se od 27. veljače 2025.

Poglavlje IV. i Prilog V. primjenjuju se od dana stupanja na snagu ove Uredbe.

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

Sastavljeno u Bruxellesu 31. siječnja 2024.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG I.

Tehničke domene i specifikacije najsuvremenijih tehnika

1. Tehničke domene na razini AVA_VAN 4 ili 5:

   (a) dokumenti koji se odnose na usklađenu evaluaciju tehničke domene „pametne kartice i slični uređaji”, a posebno sljedeći dokumenti u verzijama na snazi [datum stupanja na snagu]:

      1. „Minimalni zahtjevi ITSEF-a za sigurnosne evaluacije pametnih kartica i sličnih uređaja”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      2. „Minimalni sigurnosni zahtjevi za lokaciju”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      3. „Primjena zajedničkih kriterija na integrirane krugove”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      4. „Zahtjevi za sigurnosnu arhitekturu (ADV_ARC) za pametne kartice i slične uređaje”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      5. „Certifikacija proizvoda s ‚otvorenom’ tehnologijom pametnih kartica”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      6. „Evaluacija složenih proizvoda za pametne kartice i slične uređaje”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      7. „Primjena potencijala za napad na pametne kartice”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;

   (b) dokumenti koji se odnose na usklađenu evaluaciju tehničke domene „hardverski uređaji sa sigurnosnim kutijama”, a posebno sljedeći dokumenti u verzijama na snazi [datum stupanja na snagu]:

      1. „Minimalni zahtjevi za ITSEF za sigurnosne evaluacije hardverskih uređaja sa sigurnosnim kutijama”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      2. „Minimalni sigurnosni zahtjevi za lokaciju”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;
      3. „Primjena potencijala za napad na hardverske uređaje sa sigurnosnim kutijama”, dokument koji je ECCG izvorno odobrio 20. listopada 2023.;

2. Specifikacije najsuvremenijih tehnika u verziji na snazi [datum stupanja na snagu]:

   (a) dokument koji se odnosi na usklađenu akreditaciju tijela za ocjenjivanje sukladnosti: „Akreditacija ITSEF-a za EUCC”, koji je ECCG prvotno odobrio 20. listopada 2023.

PRILOG II.

Profili zaštite certificirani na razini AVA_VAN 4 ili 5:

1. Za kategoriju kvalificiranih sredstava za udaljenu izradu elektroničkih potpisa i pečata:

1. EN 419241-2:2019 – Vjerodostojni sustavi za potporu potpisivanja na poslužitelju – 2. dio: Profil zaštite za kvalificirano sredstvo za izradu elektroničkog potpisa za potpisivanje na poslužitelju;
2. EN 419221-5:2018 – Profili zaštite kriptografskih modula pružatelja usluga povjerenja (TSP-a) – 5. dio: Kriptografski modul za usluge povjerenja

2. Profili zaštite koji su doneseni kao specifikacije najsuvremenijih tehnika:

[BLANK]

PRILOG III.

Preporučeni profili zaštite (primjeri tehničkih domena iz Priloga I.)

Profili zaštite u certifikaciji IKT proizvoda koji pripadaju sljedećim kategorijama IKT proizvoda:

(a) za kategoriju strojno čitljivih putnih isprava:

1. Profil zaštite za strojno čitljivu putnu ispravu za koju se koristi standardni postupak pregleda s PACE-om, BSI-CC-PP-0068-V2-2011-MA-01;

2. Profil zaštite za strojno čitljivu putnu ispravu s proširenom kontrolom pristupa za ICAO, BSI-CC-PP-0056-2009;

3. Profil zaštite za strojno čitljivu putnu ispravu s proširenom kontrolom pristupa za ICAO s PACE-om, BSI-CC-PP-0056-V2-2012-MA-02;

4. Profil zaštite za strojno čitljivu putnu ispravu s osnovnom kontrolom pristupa za ICAO, BSI-CC-PP-0055-2009;

(b) za kategoriju sigurnih sredstava za izradu potpisa:

1. EN 419211-1:2014 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 1. dio: Pregled

2. EN 419211-2:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 2. dio: Sredstvo za generiranje ključa;

3. EN 419211-3:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 3. dio: Sredstvo za uvođenje ključa;

4. EN 419211-4:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 4. dio: Dodatna zaštita sredstava za generiranje ključa i povjerljivi kanal do aplikacije za generiranje certifikata;

5. EN 419211-5:2013 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 5. dio: Dodatna zaštita sredstava za generiranje ključa i povjerljivi kanal do aplikacije za izradu elektroničkog potpisa;

6. EN 419211-6:2014 – Obrasci zaštite sredstava za izradu elektroničkog potpisa – 6. dio: Dodatna zaštita sredstava za uvođenje ključa i povjerljivi kanal do aplikacije za izradu elektroničkog potpisa;

(c) za kategoriju digitalnih tahografa:

1. Digitalni tahograf – tahografska kartica iz Provedbene uredbe Komisije (EU) 2016/799 od 18. ožujka 2016. o provedbi Uredbe (EU) br. 165/2014 (Prilog 1.C);

2. Digitalni tahograf – jedinica u vozilu iz Priloga I.B Uredbi Komisije (EZ) br. 1360/2002 namijenjena za ugradnju u vozila za cestovni prijevoz;

3. Digitalni tahograf – vanjski uređaj GNSS-a (PZ za EGP) iz Priloga 1.C Provedbenoj uredbi Komisije (EU) 2016/799 od 18. ožujka 2016. o provedbi Uredbe (EU) br. 165/2014 Europskog parlamenta i Vijeća;

4. Digitalni tahograf – senzor kretanja (PZ za MS) iz Priloga 1.C Provedbenoj uredbi Komisije (EU) 2016/799 od 18. ožujka 2016. o provedbi Uredbe (EU) br. 165/2014 Europskog parlamenta i Vijeća;

(d) za kategoriju sigurnih integriranih krugova, pametnih kartica i s njima povezanih uređaja:

1. Profil zaštite za platformu sigurnosnog integriranog kruga, BSI-CC-PP-0084-2014;

2. Sustav Java Card – otvorena konfiguracija, V3.0.5 BSI-CC-PP-0099-2017;

3. Sustav Java Card – zatvorena konfiguracija, BSI-CC-PP-0101-2017;

4. Profil zaštite za porodicu modula u skladu sa standardom Trusted Platform Module za klijentsko osobno računalo 2.0, razina 0, revizija 1.16, ANSSI-CC-PP-2015/07;

5. Univerzalna SIM kartica, PU-2009-RT-79, ANSSI-CC-PP-2010/04;
6. Ugrađeni UICC (eUICC) za uređaje koji izravno komuniciraju s drugim strojevima, BSI-CC-PP-0089-2015;

(e) za kategoriju točaka interakcije (za plaćanja) i terminala za plaćanje:

1. Točka interakcije „POI-CHIP-ONLY”, ANSSI-CC-PP-2015/01;
2. Točka interakcije „POI-CHIP-ONLY i paket otvorenog protokola”, ANSSI-CC-PP-2015/02;
3. Točka interakcije „POI-COMPREHENSIVE”, ANSSI-CC-PP-2015/03;
4. Točka interakcije „POI-COMPREHENSIVE i paket otvorenog protokola”, ANSSI-CC-PP-2015/04;
5. Točka interakcije „POI-PED-ONLY”, ANSSI-CC-PP-2015/05;
6. Točka interakcije „POI-PED-ONLY i paket za otvoreni protokol”, ANSSI-CC-PP-2015/06;

(f) za kategoriju hardverskih uređaja sa sigurnosnim kutijama:

1. Kriptografski modul za operacije potpisivanja pružatelja kriptografskih usluga sa sigurnosnom kopijom – PP CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;
2. Kriptografski modul za usluge generiranja ključeva pružatelja kriptografskih usluga – PP CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;
3. Kriptografski modul za operacije potpisivanja pružatelja kriptografskih usluga bez sigurnosne kopije – PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

PRILOG IV.

KONTINUITET JAMSTVA I REVIZIJA CERTIFIKATA

IV.1 **Kontinuitet jamstva: područje primjene**

1. Zahtjevi u pogledu kontinuiteta jamstva navedeni u nastavku primjenjuju se na aktivnosti održavanja povezane s:

   (a) ponovnom procjenom ispunjava li nepromijenjeni certificirani IKT proizvod i dalje sigurnosne zahtjeve;

   (b) evaluacijom kako promjene certificiranog IKT proizvoda utječu na njegovu certifikaciju;

   (c) primjenom zakrpi u skladu s ocijenjenim postupkom upravljanja zakrpama, ako je taj postupak uključen u certifikaciju.

   (d) revizijom procesa upravljanja životnim ciklusom odnosno proizvodnje koje provodi nositelj certifikata, ako su ti procesi uključeni u certifikaciju.

2. Nositelj EUCC certifikata može zatražiti reviziju certifikata u sljedećim slučajevima:

   (a) EUCC certifikat istječe za devet mjeseci ili manje;

   (b) došlo je do promjene certificiranog IKT proizvoda ili drugog faktora koja može utjecati na sigurnosnu funkcionalnost proizvoda;

   (c) nositelj certifikata zahtijeva da se ponovno provede procjena ranjivosti kako bi se ponovno potvrdilo jamstvo EUCC certifikata povezano s otpornošću IKT proizvoda na postojeće kibernetičke napade.

IV.2 **Ponovna procjena**

1. Ako je potrebno procijeniti kako promjene prijetnji utječu na nepromijenjeni certificirani IKT proizvod, certifikacijskom tijelu podnosi se zahtjev za ponovnu procjenu.

2. Ponovnu procjenu radi isti ITSEF koji je bio uključen u prethodnu evaluaciju, pri čemu koristi sve postojeće rezultate koji još vrijede. Fokus evaluacije mora biti na aktivnostima osiguravanja jamstva na koje bi mogla utjecati promjena prijetnji certificiranom IKT proizvodu, osobito na relevantnoj porodici AVA_VAN i porodici životnog ciklusa jamstva (ALC), u okviru koje se ponovno prikupljaju dostatni dokazi o održavanju razvojnog okruženja.

3. ITSEF ažurira prethodno tehničko izvješće o evaluaciji unošenjem opisa promjena i detaljnih rezultata ponovne procjene.

4. Certifikacijsko tijelo pregledava ažurirano tehničko izvješće o evaluaciji i sastavlja izvješće o ponovnoj procjeni. Zatim se status početnog certifikata mijenja u skladu s člankom 13.

5. Izvješće o ponovnoj procjeni i ažurirani certifikat dostavljaju se nacionalnom tijelu za kibernetičkosigurnosnu certifikaciju te ENISA-i radi objave na njezinim internetskim stranicama o kibernetičkosigurnosnoj certifikaciji.

IV.3. **Promjene certificiranog IKT proizvoda**

1. U slučaju promjena certificiranog IKT proizvoda nositelj certifikata koji želi zadržati certifikat dostavlja certifikacijskom tijelu izvješće o analizi utjecaja.

2. U izvješću o analizi utjecaja navode se sljedeći elementi:

   (a) uvod s informacijama potrebnima za identifikaciju izvješća o analizi utjecaja i predmeta evaluacije koji je promijenjen;

(b) opis promjena proizvoda;

(c) upućivanja na pojedinačne proizvođačeve dokaze koji su pod utjecajem;

(d) opis izmjena proizvođačevih dokaza;

(e) nalaze i zaključke o učinku na sigurnosno jamstvo za svaku promjenu.

3. Certifikacijsko tijelo ispituje promjene opisane u izvješću o analizi utjecaja kako bi potvrdilo utjecaj tih promjena na sigurnosno jamstvo certificiranog predmeta evaluacije, kako je predloženo u zaključcima izvješća o analizi učinka.

4. Nakon ispitivanja certifikacijsko tijelo kvalificira razmjere promjene kao manje ili veće s obzirom na njezin utjecaj.

5. Ako certifikacijsko tijelo potvrdi da je riječ o manjim promjenama, izdaje se novi certifikat za izmijenjeni IKT proizvod i sastavlja se izvješće o održavanju uz izvješće o početnoj certifikaciji pod sljedećim uvjetima:

(a) izvješće o održavanju uvrštava se kao podskup izvješća o analizi utjecaja i sadržava sljedeće odjeljke:

1. uvod;

2. opis promjena;

3. pojedinačni proizvođačevi dokazi koji su pod utjecajem;

(b) rok valjanosti novog certifikata ne smije biti dulji od datuma početnog certifikata.

6. Novi certifikat, zajedno s izvješćem o održavanju, dostavlja se ENISA-i radi objave na njezinim internetskim stranicama za kibernetičkosigurnosnu certifikaciju.

7. Ako se potvrdi da je riječ o većim promjenama, provodi se ponovna evaluacija u kontekstu prethodne evaluacije, pri čemu koriste svi postojeći rezultati prethodne evaluacije koji su još relevantni.

8. Nakon dovršetka evaluacije promijenjenog predmeta evaluacije ITSEF sastavlja novo tehničko izvješće o evaluaciji. Certifikacijsko tijelo pregledava ažurirano tehničko izvješće o evaluaciji i, prema potrebi, izdaje novi certifikat s novim izvješćem o certifikaciji.

9. Novi certifikat i izvješće o certifikaciji dostavljaju se ENISA-i radi objave.

IV.4 **Upravljanje zakrpama**

1. Postupak upravljanja zakrpama omogućuje odvijanje strukturiranog procesa ažuriranja certificiranog IKT proizvoda. Postupak upravljanja zakrpama, uključujući mehanizam koji je podnositelj zahtjeva za certifikaciju ugradio u IKT proizvod, može se koristiti nakon certifikacije IKT proizvoda pod odgovornošću tijela za ocjenjivanje sukladnosti.

2. Podnositelj zahtjeva za certifikaciju može u certifikaciju IKT proizvoda uključiti mehanizam za primjenu zakrpi kao dio certificiranog postupka upravljanja koji je dio IKT proizvoda pod jednim od sljedećih uvjeta:

(a) funkcionalnosti na koje utječe zakrpa nisu predmet evaluacije certificiranog IKT proizvoda;

(b) zakrpa se odnosi na unaprijed određenu manju promjenu certificiranog IKT proizvoda;

(c) zakrpa se odnosi na potvrđenu ranjivost s kritičnim utjecajem na sigurnost certificiranog IKT proizvoda.

3. Ako se zakrpa odnosi na veću promjenu predmeta evaluacije certificiranog IKT proizvoda u odnosu na prethodno neotkrivenu ranjivost bez kritičnog utjecaja na sigurnost IKT proizvoda, primjenjuju se odredbe članka 13.

4. Postupak upravljanja zakrpama IKT proizvoda sastoji se od sljedećih elemenata:

   (a) procesa razvoja i objavljivanja zakrpa za IKT proizvod;

   (b) tehničkog mehanizma i funkcija za primjenu zakrpe na IKT proizvod;

   (c) skupa evaluacijskih aktivnosti povezanih s djelotvornošću i radom tehničkog mehanizma.

5. Tijekom certifikacije IKT proizvoda:

   (a) podnositelj zahtjeva za certifikaciju IKT proizvoda dostavlja opis postupka upravljanja zakrpama;

   (b) ITSEF provjerava:

      1. da je proizvođač ugradio mehanizme za zakrpe u IKT proizvod u skladu s postupkom upravljanja zakrpama podnesenim na certifikaciju;

      2. da su granice predmeta evaluacije tako da promjene u zasebnim procesima ne utječu na sigurnost predmeta evaluacije;

      3. da tehnički mehanizam za zakrpe funkcionira u skladu s odredbama ovog odjeljka i tvrdnjama podnositelja zahtjeva;

   (c) certifikacijsko tijelo unosi ishod ocijenjenog postupka upravljanja zakrpama u izvješće o certifikaciji.

6. Nositelj certifikata može primijeniti zakrpu izrađenu u skladu s certificiranim postupkom upravljanja zakrpama na predmetni certificirani IKT proizvod pa u roku od pet radnih dana poduzima sljedeće korake u ovim slučajevima:

   (a) u slučaju iz točke 2. podtočke (a) zakrpu prijavljuje certifikacijskom tijelu, koje ne mijenja odgovarajući EUCC certifikat;

   (b) u slučaju iz točke 2. podtočke (b) zakrpu podnosi ITSEF-u na pregled. ITSEF nakon primitka zakrpe obavješćuje certifikacijsko tijelo nakon čega certifikacijsko tijelo poduzima odgovarajuće radnje radi izdavanja nove verzije odgovarajućeg EUCC certifikata i ažuriranju izvješća o certifikaciji;

   (c) u slučaju iz točke 2. podtočke (c) zakrpu podnosi ITSEF-u kako bi se provela potrebna ponovna evaluacija, ali je istodobno može primijeniti. ITSEF obavješćuje certifikacijsko tijelo nakon čega ono počinje obavljati relevantne poslove certifikacije.

PRILOG V.

SADRŽAJ IZVJEŠĆA O CERTIFIKACIJI

V.1. **Izvješće o certifikaciji**

1. Certifikacijsko tijelo na temelju tehničkih izvješća o evaluaciji koje dostavlja ITSEF sastavlja izvješće o certifikaciji koje se objavljuje zajedno s odgovarajućim EUCC certifikatom.

2. Izvješće o certifikaciji je referencija s detaljnim i praktičnim informacijama o IKT proizvodu ili kategoriji IKT proizvoda i o sigurnom stavljanju IKT proizvoda u upotrebu, pa mora sadržavati sve javno dostupne i objavljive informacije koje su relevantne korisnicima i zainteresiranim stranama. Izvješće o certifikaciji može sadržavati upućivanja na javno dostupne i objavljive informacije.

3. Izvješće o certifikaciji mora sadržavati barem sljedeće elemente:

   (a) sažetak;

   (b) informacije o kojem je IKT proizvodu ili, u slučaju profila zaštite, kategoriji IKT proizvoda riječ;

   (c) sigurnosne usluge;

   (d) pretpostavke i objašnjenje opsega;

   (e) informacije o arhitekturi;

   (f) prema potrebi, dodatne informacije o kibernetičkoj sigurnosti;

   (g) ispitivanje IKT proizvoda, ako je provedeno;

   (h) prema potrebi, informacije o tome koje procese upravljanja životnim ciklusom i proizvodne objekte koristi nositelj certifikata;

   (i) rezultate evaluacije i informacije o certifikatu;

   (j) sažetak potrebne sigurnosti IKT proizvoda podnesenog na certifikaciju;

   (k) ako su dostupni, oznaku ili etiketu povezane s programom;

   (l) bibliografiju.

4. Sažetak je kratak sažetak cjelokupnog izvješća o certifikaciji. U njemu se daje jasan i jezgrovit pregled rezultata evaluacije i mora sadržavati sljedeće informacije:

   (a) ime evaluiranog IKT proizvoda, popis komponenti proizvoda uključenih u evaluaciju i verziju IKT proizvoda;

   (b) ime ITSEF-a koji je proveo evaluaciju i, prema potrebi, popis podugovaratelja;

   (c) datum završetka evaluacije;

   (d) upućivanje na tehničko izvješće o evaluaciji koje je sastavio ITSEF;

   (e) kratak opis rezultata iz izvješća o certifikaciji, uključujući:

      1. verziju i, prema potrebi, izdanje zajedničkih kriterija primijenjenih u evaluaciji;

      2. sigurnosni jamstveni paket i komponente sigurnosnog jamstva zajedničkih kriterija, uključujući razinu AVA_VAN, primijenjene u evaluaciji i odgovarajuću jamstvenu razinu iz članka 52. Uredbe (EU) 2019/881 na koju se odnosi EUCC certifikat;

      3. sigurnosnu funkcionalnost evaluiranog IKT proizvoda;

      4. sažetak prijetnji i organizacijskih sigurnosnih politika za koje je namijenjen evaluirani IKT proizvod;

5. posebne konfiguracijske zahtjeve;

6. pretpostavke o radnom okruženju;

7. prema potrebi, postoji li odobreni postupak upravljanja zakrpama u skladu s odjeljkom IV.4. Priloga IV.;

8. izjave o ograničenju odgovornosti.

5. Evaluirani IKT proizvod mora biti jasno identificiran, što obuhvaća sljedeće:

(a) ime evaluiranog IKT proizvoda;

(b) popis komponenti IKT proizvoda uključenih u evaluaciju;

(c) broj verzije komponenti IKT proizvoda;

(d) navođenje dodatnih zahtjeva za radno okruženje certificiranog IKT proizvoda;

(e) ime i podaci za kontakt nositelja EUCC certifikata;

(f) prema potrebi, postupak upravljanja zakrpama uvršten u certifikat;

(g) poveznica na internetske stranice nositelja EUCC certifikata na kojima su navedene dodatne informacije o kibernetičkoj sigurnosti certificiranog IKT proizvoda u skladu s člankom 55. Uredbe (EU) 2019/881.

6. Informacije iz ovog odjeljka moraju biti što točnije kako bi se dobio potpun i točan prikaz IKT proizvoda koji se može ponovno iskoristiti u budućim evaluacijama.

7. Odjeljak o sigurnosnoj politici mora sadržavati opis sigurnosne politike IKT proizvoda i politika ili pravila koje taj IKT proizvod mora primjenjivati ili s kojima mora biti sukladan. U njemu se navode i opisuju sljedeće politike:

(a) politika postupanja s ranjivostima nositelja certifikata;

(b) politika kontinuiteta jamstva nositelja certifikata.

8. Prema potrebi, politika može obuhvaćati uvjete koji se odnose na primjenu postupka upravljanja zakrpama tijekom valjanosti potvrde.

9. Odjeljak o pretpostavkama i objašnjenjima opsega mora sadržavati potpune informacije o okolnostima i ciljevima povezanima s namjenom proizvoda iz članka 7. stavka 1. točke (c). Te informacije obuhvaćaju:

(a) pretpostavke za korištenje i uvođenje IKT proizvoda u obliku minimalnih zahtjeva, npr. da su ispunjeni zahtjevi koji se odnose na pravilnu instalaciju i konfiguraciju te hardver;

(b) pretpostavke za okruženje za rad IKT proizvoda u skladu sa zahtjevima;

10. Informacije pod točkom 9. moraju biti što razumljivije kako bi korisnici certificiranog IKT proizvoda mogli donositi utemeljene odluke o rizicima povezanima s njegovom upotrebom.

11. Odjeljak o informacijama o arhitekturi mora sadržavati opis IKT proizvoda i njegovih glavnih komponenti više razine u skladu s porodicom za dizajn podsustava ADV_TDS iz zajedničkih kriterija.

12. Potpun popis dodatnih informacija o kibernetičkoj sigurnosti IKT proizvoda dostavlja se u skladu s člankom 55. Uredbe (EU) 2019/881. Sva relevantna dokumentacija označava se brojevima verzija.

13. Odjeljak o ispitivanju IKT proizvoda mora sadržavati sljedeće informacije:

(a) ime i točku za kontakt tijela koje je izdalo certifikat, uključujući odgovorno nacionalno tijelo za kibernetičkosigurnosnu certifikaciju;

(b) ime ITSEF-a koji je proveo evaluaciju, ako se razlikuje od certifikacijskog tijela;

(c) identifikacijske podatke o primijenjenim jamstvenim komponentama iz normi iz članka 3.;

(d) verziju specifikacije najsuvremenijih tehnika i dodatne kriterije za evaluaciju sigurnosti korištene u evaluaciji;

(e) potpune i točne postavke i konfiguraciju IKT proizvoda tijekom evaluacije, uključujući operativne napomene i opažanja ako ih ima;

(f) korišteni profili zaštite, što uključuje sljedeće informacije:

1. autor profila zaštite;

2. ime i identifikacijska oznaka profila zaštite;

3. identifikacijska oznaka certifikata profila zaštite;

4. ime i podatke za kontakt certifikacijskog tijela i ITSEF-a uključenog u evaluaciju profila zaštite;

5. jamstvene pakete potrebne za proizvod sukladan s profilom zaštite.

14. Rezultati evaluacije i informacije za odjeljak o certifikatu moraju obuhvaćati:

(a) potvrdu postignute jamstvene razine iz članka 4. ove Uredbe i članka 52. Uredbe (EU) 2019/881;

(b) zahtjeve za sigurnosno jamstvo iz normi iz članka 3. koje IKT proizvod ili profil zaštite stvarno ispunjava, uključujući razinu AVA_VAN;

(c) detaljan opis zahtjeva za sigurnosno jamstvo, kao i pojedinosti o tome kako proizvod ispunjava svaki od njih;

(d) datum izdavanja i razdoblje valjanosti certifikata;

(e) jedinstvenu identifikacijsku oznaku certifikata.

15. Potrebna sigurnost uvrštava se u izvješće o certifikaciji u cijelosti ili kao sažetak s upućivanjem te se za potrebe objave povezuje s tim izvješćem.

16. Potrebna sigurnost može se pročistiti u skladu s odjeljkom VI.2.

17. Oznaka ili etiketa povezana s EUCC-om može se unijeti u izvješće o certifikaciji u skladu s pravilima i postupcima iz članka 11.

18. Odjeljak o bibliografiji mora sadržavati upućivanja na sve dokumente koji su poslužili u sastavljanju izvješća o certifikaciji. Te informacije uključuju barem sljedeće:

(a) kriterije za evaluaciju sigurnosti, specifikacije najsuvremenijih tehnika i druge relevantne korištene specifikacije te njihovu verziju;

(b) tehničko izvješće o evaluaciji;

(c) prema potrebi, tehničko izvješće o evaluaciji za složenu evaluaciju;

(d) tehničku referentnu dokumentaciju;

(e) proizvođačevu dokumentaciju korištenu u evaluacijskom radu.

19. Kako bi se zajamčila obnovljivost evaluacije, sva navedena dokumentacija mora biti jedinstveno označena ispravnim datumom izdanja i ispravnim brojem verzije.

V.2. **Pročišćavanje potrebne sigurnosti za objavu**

1. Potrebna sigurnost koja se uvrštava u izvješće o certificiranju ili na koju se upućuje u tom izvješću u skladu s točkom 1. odjeljkom VI.1. može se pročistiti uklanjanjem ili parafraziranjem vlasničkih tehničkih informacija.

2. Dobivena pročišćena potrebna sigurnost mora biti stvarna reprezentacija cijelog njezina izvornog oblika. To znači da se u pročišćenoj potrebnoj sigurnosti ne smiju izostaviti informacije potrebne za razumijevanje sigurnosnih svojstava predmeta evaluacije i opsega evaluacije.

3. Sadržaj pročišćene potrebne sigurnosti mora biti u skladu sa sljedećim minimalnim zahtjevima:
   (a) uvod se ne smije pročišćavati jer načelno ne uključuje vlasničke informacije;
   (b) pročišćena potrebna sigurnost mora imati jedinstvenu identifikacijsku oznaku koja se razlikuje od oznake cijelog njezina izvornog oblika;
   (c) opis predmeta evaluacije može se skratiti jer može sadržavati vlasničke i detaljne informacije o dizajnu predmeta evaluacije koje ne bi trebale biti objavljene;
   (d) opis sigurnosnog okruženja predmeta evaluacije (pretpostavke, prijetnje, organizacijske sigurnosne politike) ne smije se skraćivati ako su te informacije potrebne za razumijevanje opsega evaluacije;
   (e) sigurnosni ciljevi ne smiju se skraćivati se jer se sve informacije moraju objaviti da bi se razumjela namjera potrebne sigurnosti i predmeta evaluacije;
   (f) svi se sigurnosni zahtjevi moraju objaviti. U napomenama uz prijavu mogu se navesti informacije o tome kako su funkcionalni zahtjevi iz zajedničkih kriterija iz članka 3. iskorišteni da bi se razumjela potrebna sigurnost;
   (g) sažetak specifikacije predmeta evaluacije mora sadržavati sve sigurnosne funkcije predmeta evaluacije, ali dodatne vlasničke informacije mogu se pročistiti;
   (h) navode se upućivanja na profile zaštite primijenjene na predmet evaluacije;
   (i) obrazloženje se može pročistiti tako da se uklone vlasničke informacije.

4. Čak i ako pročišćena potrebna sigurnost nije službeno evaluirana u skladu s evaluacijskim normama iz članka 3., certifikacijsko tijelo dužno se pobrinuti da je ona u skladu s potpunom i evaluiranom potrebnom sigurnosti te u izvješću o certifikaciji navodi potpunu i pročišćenu potrebnu sigurnost.

PRILOG VI.

OPSEG I SASTAV TIMA ZA ISTORAZINSKO OCJENJIVANJE

VI.1. **Opseg istorazinskog ocjenjivanja**

1. Obuhvaćene su sljedeće vrste istorazinskog ocjenjivanja:

   (a) 1. vrsta: certifikacijsko tijelo obavlja certifikacijske aktivnosti na razini AVA_VAN.3;

   (b) 2. vrsta: certifikacijsko tijelo obavlja certifikacijske aktivnosti koje se odnose na tehničku domenu navedenu kao specifikacija najsuvremenijih tehnika u Prilogu I.;

   (c) 3. vrsta: certifikacijsko tijelo obavlja certifikacijske aktivnosti na razinama višim od AVA_VAN.3, pri čemu koristi profil koji je u Prilogu II. ili III. naveden kao specifikacija najsuvremenijih tehnika.

2. Certifikacijsko tijelo koje se istorazinski ocjenjuje podnosi popis certificiranih IKT proizvoda koji mogu biti kandidati za pregled tima za istorazinsko ocjenjivanje u skladu sa sljedećim pravilima:

   (a) proizvodi kandidati pokrivaju tehnički opseg autorizacije certifikacijskog tijela, pri čemu će se u istorazinskom ocjenjivanju analizirati evaluacije na visokoj jamstvenoj razini za najmanje dva različita proizvoda i jedan profil zaštite ako je certifikacijsko tijelo izdalo certifikat s visokom jamstvenom razinom;

   (b) za istorazinsko ocjenjivanje 2. vrste certifikacijsko tijelo podnosi najmanje jedan proizvod po tehničkoj domeni i predmetnom ITSEF-u;

   (c) za istorazinsko ocjenjivanje 3. vrste evaluira se najmanje jedan proizvod kandidat u skladu s primjenjivim i relevantnim profilima zaštite.

VI.2 **Tim za istorazinsko ocjenjivanje**

1. Ocjenjivački tim sastoji se od najmanje dva stručnjaka odabranih iz različitih certifikacijskih tijela iz različitih država članica koja izdaju certifikate s visokom jamstvenom razinom. Stručnjaci bi trebali dokazati relevantno stručno poznavanje normi iz članka 3. i specifikacija najsuvremenijih tehnika u opsegu istorazinskog ocjenjivanja.

2. U slučaju delegiranja izdavanja certifikata ili prethodnog odobrenja certifikata iz članka 56. stavka 6. Uredbe (EU) 2019/881 stručnjak iz nacionalnog tijela za kibernetičkosigurnosnu certifikaciju povezan s predmetnim certifikacijskim tijelom mora sudjelovati i u timu stručnjaka odabranih u skladu sa stavkom 1. ovog odjeljka.

3. Za istorazinsko ocjenjivanje 2. vrste članovi tima odabiru se iz certifikacijskih tijela koja su ovlaštena za tu tehničku domenu.

4. Svaki član ocjenjivačkog tima mora imati najmanje dvije godine iskustva u obavljanju certifikacijskih aktivnosti u certifikacijskom tijelu.

5. Za istorazinsko ocjenjivanje 2. ili 3. vrste svaki član ocjenjivačkog tima mora imati najmanje dvije godine iskustva u obavljanju certifikacijskih aktivnosti u relevantnoj tehničkoj domeni ili profilu zaštite te dokazano stručno znanje i sudjelovanje u autorizaciji nekog ITSEF-a.

6. Nacionalno tijelo za kibernetičkosigurnosnu certifikaciju koje prati i nadzire certifikacijsko tijelo koje se istorazinski ocjenjuje i najmanje jedno nacionalno tijelo za kibernetičkosigurnosnu certifikaciju čije certifikacijsko tijelo ne podliježe istorazinskom ocjenjivanju sudjeluju u istorazinskom ocjenjivanju kao promatrači. ENISA također može sudjelovati u istorazinskom ocjenjivanju kao promatrač.

7. Certifikacijskom tijelu koje se istorazinski ocjenjuje daje se na uvid sastav tima za istorazinsko ocjenjivanje. Ono u opravdanim slučajevima može osporiti sastav tima za istorazinsko ocjenjivanje i zatražiti da se taj sastav ponovno razmotri.

PRILOG VII.

Sadržaj EUCC certifikata

EUCC certifikat mora sadržavati barem:

(a) jedinstvenu identifikacijsku oznaku koji je odredilo certifikacijsko tijelo koje je izdalo certifikat;

(b) informacije o certificiranom IKT proizvodu ili profilu zaštite i nositelju certifikata, uključujući:

1. ime IKT proizvoda ili profila zaštite i, prema potrebi, predmeta evaluacije;
2. vrstu IKT proizvoda ili profila zaštite i, prema potrebi, predmeta evaluacije;
3. verziju IKT proizvoda ili profila zaštite;
4. ime, adresu i podatke za kontakt nositelja certifikata;
5. poveznicu na internetske stranice nositelja certifikata s dodatnim informacijama o kibernetičkoj sigurnosti iz članka 55. Uredbe (EU) 2019/881;

(c) informacije povezane s evaluacijom i certifikacijom IKT proizvoda ili profila zaštite, uključujući:

1. ime, adresu i podatke za kontakt certifikacijskog tijela koje je izdalo certifikat;
2. ime ITSEF-a koji je proveo evaluaciju ako se razlikuje od certifikacijskog tijela,
3. ime odgovornog nacionalnog tijela za kibernetičkosigurnosnu certifikaciju;
4. upućivanje na ovu Uredbu;
5. upućivanje na izvješće o certifikaciji povezano s certifikatom iz Priloga V.;
6. primjenjivu jamstvenu razinu u skladu s člankom 4.;
7. upućivanje na verziju normi iz članka 3. korištenih u evaluaciji;
8. podatke za identifikaciju jamstvene razine ili paketa specificiranih u normama iz članka 3. i u skladu s Prilogom VIII., uključujući primijenjene jamstvene komponente i obuhvaćenu razinu AVA_VAN;
9. prema potrebi, upućivanje na profile zaštite s kojima je IKT proizvod ili profil zaštite sukladan;
10. datum izdavanja;
11. razdoblje valjanosti certifikata;

(d) oznaku i etiketu povezane s certifikatom u skladu s člankom 11.

PRILOG VIII.

Deklaracija jamstvenog paketa

1. Suprotno definicijama iz zajedničkih kriterija, proširenje:

(a) ne smije imati oznaku „+”;

(b) mora biti precizirano popisom svih komponenti na koje se odnosi;

(c) mora biti detaljno opisano u izvješću o certifikaciji.

2. Jamstvena razina potvrđena u EUCC certifikatu može se dopuniti jamstvenom razinom evaluacije kako je navedeno u članku 3. ove Uredbe.

3. Ako se jamstvena razina koja je potvrđena u EUCC certifikatu ne odnosi na proširenje, u EUCC certifikatu navodi se jedan od sljedećih paketa:

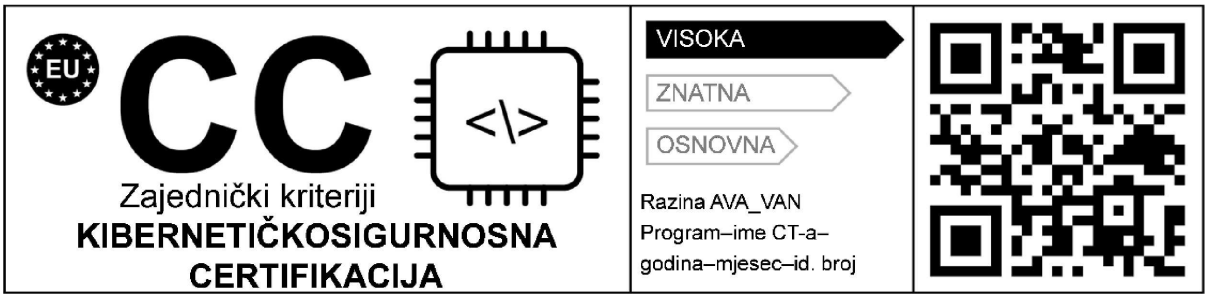
(a) „specifični jamstveni paket”;

(b) „jamstveni paket sukladan profilu zaštite” u slučaju navođenja profila zaštite bez jamstvene razine evaluacije.

PRILOG IX.

Znak i oznaka

1. Oblik znaka i oznake:



2. Ako se znak i oznaka smanje ili povećaju, moraju se zadržati proporcije iz gornjeg crteža.

3. Visina fizičkog znaka i oznake mora biti najmanje 5 mm.