

Az uniós kiberbiztonsági tanácsot keret

Az IKT-termékek uniós kiberbiztonsági tanácsot keretrendszerére lehetőséget tesz a tesztelésre szabott és kockázatalapú uniós tanácsot keretrendszerek létrehozására.



© iStock by Getty Images -1159281243 Wojtek Skora

A tanácsot keretrendszer kulcsfontosságú szerepet játszik a digitális világ számára fontos termékekbe és szolgáltatásokba vetett bizalom és biztonság növelésében. Jelenleg az EU-ban számos kiberbiztonsági tanácsot keretrendszer létezik az IKT-termékekre vonatkozóan. Az EU-szerte érvényes kiberbiztonsági tanácsot keretrendszerre vonatkozó kockázati keret hiányában azonban egyre nagyobb a szóttagoltság és a tagállamok közötti akadályok kockázata.

A tanácsot keretrendszer az egész EU-ra kiterjedő tanácsot keretrendszereket fog biztosítani, mint átfogó szabályrendszert, műszaki követelményeket, szabványokat és eljárásokat. A keret egy adott IKT-alapú termék vagy szolgáltatás biztonsági tulajdonságainak értékeléséről szóló, uniós szinten megállapodáson fog alapulni. Tanácsot keretrendszerrel, hogy az ilyen rendszerrel összhangban tanácsot keretrendszer IKT-termékek és -szolgáltatások megfelelnek a meghatározott követelményeknek.

Minden egyes európai rendszernek meg kell határoznia kockázati szinten a következőket:

- az érintett termékek és szolgáltatások kategóriái;
- a kiberbiztonsági követelmények, például szabványok vagy műszaki eljárások;
- az értékelés típusa, például a kockázati értékelés vagy harmadik fél;
- a biztonság tervezett szintje.

A biztonsági szinteket arra használják, hogy tájékoztassák a felhasználókat a termék kiberbiztonsági kockázatairól, és alapvető, jelentős és/vagy magasak lehetnek. Árnyosak a termék, a szolgáltatás vagy a folyamat tervezett használatához kapcsolódó kockázati szinttel a baleset valószínűsége és hatása tekintetében. A magas biztonsági szint azt jelenti, hogy a tanácsot keretrendszer termék megfelelt a legmagasabb biztonsági teszteknek.

A kapott tanácsot keretrendszer valamennyi uniós tagállamban elismerik, ami megkönnyíti a vállalkozások számára a határon átnyúló kereskedelmet, a vállalkozások számára pedig a termék vagy szolgáltatás biztonsági jellemzőinek megértését.

Ami a tanácsot keretrendszer végrehajtását illeti, az [Európai Kiberbiztonsági Tanácsot keretrendszer Csoportban \(ECCG\)](#) állszegyelet tagállami hatóságok máris több alkalommal találkoztak.

Árdekelte felek kiberbiztonsági tanácsátási csoportja

A kiberbiztonsági törvény 2019. évi hatálybalépését követően az Európai Bizottság [pályázati felhívást](#) tett közzé az Árdekelte felek kiberbiztonsági tanácsátási csoportjának (SCCG) tagjainak kiválasztására.

Az SCCG feladata lesz, hogy tanácsot adjon a Bizottságnak és az ENISA-nak a kiberbiztonsági tanácsátással kapcsolatos stratégiai kérdésekben, és segítse a Bizottságot az uniós gárdák munkaprogram elkövetésében. Ez az Európai Bizottság által elindított első, az Árdekelte felek kiberbiztonsági tanácsátásával foglalkozó szakértői csoport.

[Kövessen a csoport munkáját](#)

Kövessen a legújabb fejleményeket és tájékozódjon arról, hogyan lehet részt venni a folyamatokban!

•

[Kövessen a Bizottság kiberbiztonsággal kapcsolatos munkáját @CyberSec_EU](#)

Legfrissebb hírek

PRESS RELEASE | 06 Február 2023

[EU-India: Új Kereskedelmi és Technológiai Tanács vezetői szerepet töltek be a digitális átalakulás, a zöld technológiák és a kereskedelem terén](#)

Az Európai Unió és India egy új Kereskedelmi és Technológiai Tanács (TTC) létrehozásával megerősítették stratégiai partneri kapcsolatukat.

PRESS RELEASE | 01 Február 2023

[Az EU és Szingapúr elindítja a digitális partnerséget](#)

Az EU és Szingapúr ma stratégiai partnerként erősíti együttműködését.

PRESS RELEASE | 16 Január 2023

[Új, szigorúbb szabályok lépnek életbe a kritikus fontosságú szervezetek és hálózatok kiber- és fizikai rezilienciájára vonatkozóan](#)

A kritikus és digitális infrastruktúrára szorosan kötött kulcsfontosságú iránymű nemrégiben lezárta hatályba, és erősíteni fogja az EU rezilienciáját az online és offline fenyegetésekkel szemben, a kibertámadásokkal szemben a biztonságos és kiberbiztonsági kockázatokig vagy a természeti katasztrófákig.

DIGIBYTE | 16 December 2022

[Kiberbiztonság: Az EU 8. párbeszédet folytat az Egyesült Államokkal](#)

2022. december 15-én az Európai Unió és az Egyesült Államok megtartotta a nyolcadik EU-USA kiberpárbeszédet

Washingtonban. Erre Oroszország Ukrajna elleni jogellenes katonai agressziója miatt drámaian megromlott kiberfenyegetési kárnyezet

A széfekben került sor, amely rávilágított arra, hogy fokozott transzatlanti együttműködésre és koordinációra van szükség a rosszindulatú kibertevékenységek megelőzése, felderítése és az azokra való reagálás érdekében, valamint kiemelte, hogy biztosítani kell a kritikus infrastruktúra biztonságát és ellenálló képességét.

[Bárhol is vagyunk: Cybersecurity](#)

Kapcsolódó tartalom

Ásszkóp

[Kiberbiztonsági politikák](#)

Az Európai Unió kényes frontokon dolgozik a kiberreziliencia előmozdítása, kommunikációnk és adataink védelme, valamint az online társadalom és gazdaság biztonságának megőrzése érdekében.

Melyedjen el alaposabban a témában

[Az európai kiberbiztonsági tanácsot vezető csoport](#)

Az Európai Kiberbiztonsági Tanácsot vezető csoportot az Európai Unió hozta létre, hogy segítse a kiberbiztonsági jogszabályi keret kidolgozását és alkalmazását.

Lásd még

[22 kiválasztott kiberbiztonsági projekt 10,9 milliárd EUR összegben](#)

Az alapvető szolgáltatók (OES), a nemzeti kiberbiztonsági tanácsok (NCCA-k) és az illetékes nemzeti hatóságok (NCA-k) azon kiválasztott pályázók közé tartoznak, akik 11 milliárd EUR finanszírozásban részesülnek az Európai Helyreállítási és Fejlesztési Eszköz 2020. évi...

[Európai Kiberbiztonsági Kompetenciafejlesztési Központ](#)

Az Európai Kiberbiztonsági Helyreállítási és Fejlesztési Központ segíti az EU-t a kiberbiztonsági technológiai és ipari kapacitások megőrzésében és fejlesztésében.

[Érdekeltelek a kiberbiztonsági tanácsot vezető csoporttal](#)

Az érdekeltelek a kiberbiztonsági tanácsot vezető csoporttal az Európai Unió hozta létre, hogy tanácsot adjon a kiberbiztonsági tanácsokkal kapcsolatos stratégiai kérdésekben.

[Az uniós kiberbiztonsági jogszabály](#)

A kiberbiztonsági jogszabály megerősíti az Európai Unió kiberbiztonsági ügynökségét (ENISA), és létrehozza a termékek és szolgáltatók kiberbiztonsági tanácsot vezető csoportját.

[Irányelv a kiberbiztonság Uniós-szerte egységesen magas szintjét biztosító közzétételről \(NIS2 irányelv\)](#)

A NIS2 irányelv az egész EU-ra kiterjedő kiberbiztonsági jogszabály. Jogi intézkedéseket biztosít a kiberbiztonság általános szintjének növelésére az EU-ban.

Source URL: <https://digital-strategy.ec.europa.eu/policies/cybersecurity-certification-framework>