Cyber Resilience Act

Rendelet a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről

(Kiberreziliencia jogszabály)

2022/0272(COD)

Egyéb szabályozók

CSA

2019-ben hatályba lépett törvény, amely fő elemei közé tartozik az ENISA állandó megbízatása, amelyet egy egységes európai rendszer bevezetése kísér, az IKT-termékek, -szolgáltatások és -folyamatok tanúsítási keretrendszere.

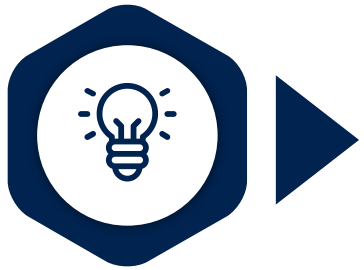
DORA

A Bizottság 2021-ben közzétette a pénzügyi szektorra vonatkozó digitális működési reziliencia rendelettervezetet, amellyel a teljes EU-s pénzügyi szektorra egységes, arányossági és kockázatalapú megközelítésen alapuló kiberbiztonsági követelményeket kíván bevezetni a fogyasztói bizalom növelése és a határon átnyúló működés megkönnyítése érdekében.

NIS 2

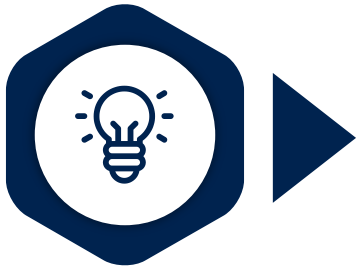
Az irányelv képezi a kiberbiztonsági kockázatkezelési intézkedések és bejelentési kötelezettségek alapját az irányelv hatálya alá tartozó valamennyi ágazatra, így az energiaszektorra, a közlekedésre, az egészségügyre és a digitális infrastruktúrára nézve.

Két fő probléma



SEBEZHETŐSÉG

- termékek alacsony kiberbiztonsági szintje
- széles körben elterjedt sebezhetőségek
- elégtelen biztonsági frissítésekhez vezetett
- többletköltségek



TERMÉKEK KIBERBIZTONSÁGA

- felhasználók megfelelő tájékoztatása
- teljes életciklusra kiterjedő kiberbiztonsági követelmények
- elégtelen biztonsági frissítések
- piacfelügyelet és végrehajtási szabályok

A jogszabály célja és hatálya

CÉLJA

- gyártók, forgalmazók szabályozása
- sebezhetőségek kezelése
- a felhasználók megfelelő tájékoztatása

HATÁLYA

- közvetlenül vagy közvetve egy másik eszközhöz vagy hálózathoz kapcsolódó eszközök
- termékek teljes életciklusára kiterjed
- kötelező kiberbiztonsági követelményeket vezet be

A jogszabály hatálya

Hatálya minden olyan termékre kiterjed, amely közvetlenül vagy közvetve egy másik eszközhöz vagy hálózathoz kapcsolódik, kivételek: például az open-source szoftverek vagy a más uniós szabályozás hatálya alá tartozó termékek (orvostechnikai eszközök, légi közlekedés, autók).

A rendelet a termékek teljes életciklusára kiterjedő kötelező kiberbiztonsági követelményeket vezet be a digitális termékek gyártóira és kereskedőire nézve, valamint a felhasználók megfelelő tájékoztatását biztosító előírásokat határoz meg.

A rendelettervezet III. melléklete meghatározza a **kritikus fontosságú termékek** körét, amelyekre különleges megfelelőségértékelési eljárás vonatkozik, és amelyek számára előírható az európai kiberbiztonsági tanúsítvány kötelező megszerzése.

Az e rendeletnek megfelelő, **digitális elemeket tartalmazó termékek forgalmazását** a tagállamok nem akadályozhatják az e rendelet hatálya alá tartozó szempontok miatt.

A rendelet meghatározza

a digitális elemeket tartalmazó termékek forgalomba hozatalára vonatkozó szabályokat az ilyen termékek kiberbiztonságának biztosítása érdekében;

a digitális elemeket tartalmazó termékek tervezésére, fejlesztésére és gyártására vonatkozó alapvető követelményeket, valamint a gazdasági szereplők e termékekkel kapcsolatos kötelezettségeit;

gyártók által a digitális elemeket tartalmazó termékek teljes életciklus alatti kiberbiztonságának biztosítása érdekében bevezetett sebezhetőségkezelési eljárásokra vonatkozó alapvető követelményeket;

a gazdasági szereplők kötelezettségeit, valamint a piacfelügyeletre és az említett szabályok és követelmények végrehajtására vonatkozó szabályokat

Biztonsági követelmények

A digitális elemekkel rendelkező termékeket úgy kell megtervezni, fejleszteni és gyártani, hogy **a kockázatok** alapján **megfelelő szintű** kiberbiztonságot biztosítsanak

A digitális elemekkel rendelkező termékeket **ismert, kihasználható sebezhetőség nélkül** kell szállítani

megfelelő ellenőrző mechanizmusokkal biztosítsa a **jogosulatlan hozzáférés elleni védelm**et, beleértve, de nem kizárólagosan a hitelesítési, identitás- vagy hozzáférés-kezelő rendszereket

a tárolt, továbbított személyes vagy egyéb **adatok bizalmasságának**, illetve a tárolt, továbbított vagy más módon feldolgozott személyes vagy egyéb adatok, parancsok, programok és konfigurációk **sértetlenségének** védelme

biztonsággal kapcsolatos információkat nyújtson a vonatkozó belső tevékenységek rögzítésével és/vagy nyomon követésével, beleértve az adatokhoz, szolgáltatásokhoz vagy funkciókhoz való hozzáférést vagy azok módosítását

Biztonsági követelmények

Biztonságos alapértelmezett konfiguráció: termék eredeti állapotba való visszaállításának lehetősége, **biztonsági frissítések automatikus telepítése**, felhasználók eltávolíthatnak minden adatot és beállítást	**Adatminimalizálás**: Csak azokat az adatokat dolgozza fel, amelyek megfelelőek, relevánsak és korlátozottak az adott termék tervezett felhasználási céljához viszonyítva	Védi az **alapvető funkciók rendelkezésre állás**át, beleértve a DDoS támadásokkal szembeni ellenállóságot és csökkentést;	Minimalizálja saját maguk vagy kapcsolt eszközeik által okozott negatív hatást **más eszközök vagy hálózatok** által nyújtott szolgáltatások rendelkezésre állására	Olyan módon legyen tervezve, fejlesztve és gyártva, hogy **minimalizálja a támadási felületeket, beleértve a külső interfészeket**

Sebezhetőségek kezelésére vonatkozó követelmények

A DIGITÁLIS ELEMEKKEL RENDELKEZŐ TERMÉKEK GYÁRTÓINAK KÖTELESSÉGE

azonosítani és dokumentálni a termékben található sebezhetőségek és a szoftveres összetevők jegyzékének elkészítését (SBoM) egy általánosan használt és géppel olvasható formátumban (függőségek azonosítása)	a digitális elemeket tartalmazó termékekkel kapcsolatos kockázatokkal kapcsolatban haladéktalanul kezelni és orvosolni a sebezhetőséget, beleértve a **biztonsági frissítéseket** is;	**hatékony és rendszeres teszteket** és felülvizsgálatokat végezni a digitális elemekkel ellátott termék biztonságáról;	amint a biztonsági frissítés elérhetővé vált, **nyilvánosságra kell hozni a javított biztonsági rések**kel kapcsolatos információkat (sérülékenységek hatásait, súlyosságukat és a felhasználókat a hiba elhárításában segítő információkat);	biztosítani, hogy amennyiben rendelkezésre állnak **biztonsági javítások vagy frissítések, azokat késedelem nélkül és ingyenesen terjesztik**, a felhasználókat a vonatkozó információkkal ellátni.

Kritikus fontosságú termékek

III. melléklet

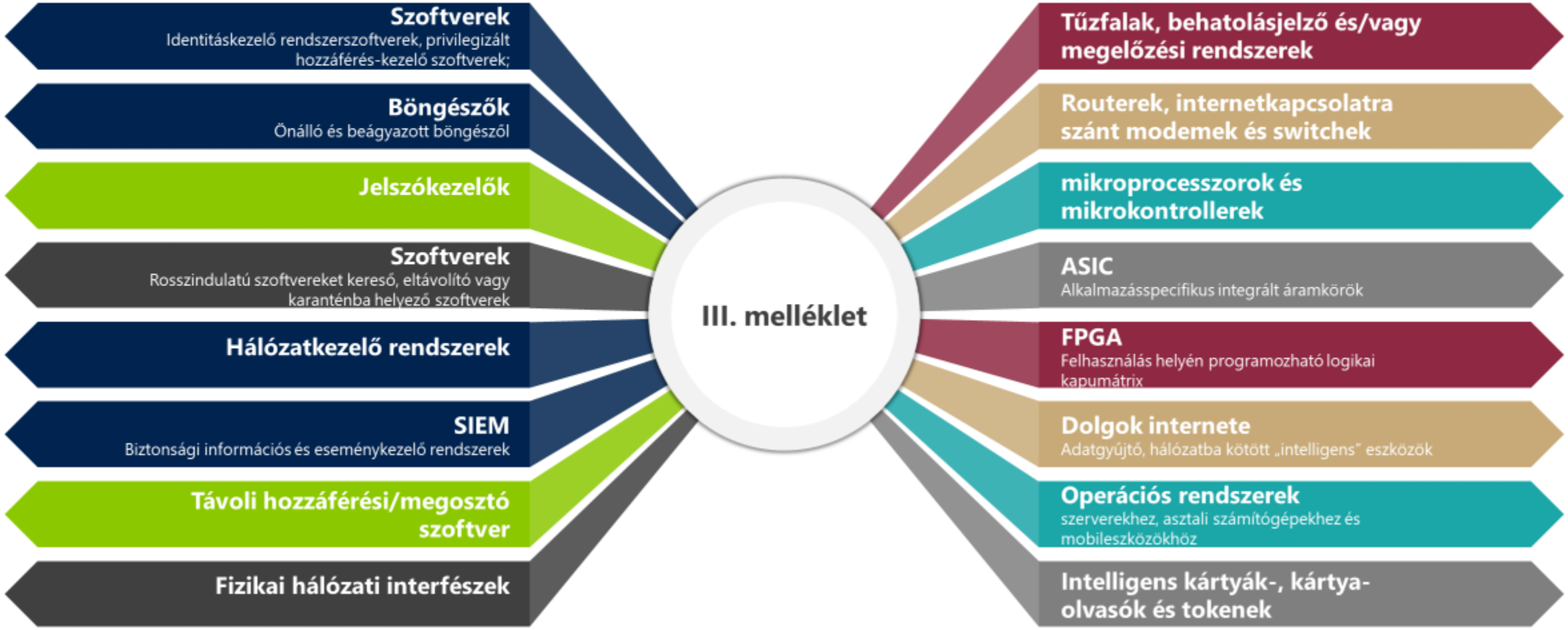
- **I. osztály**
- **II. osztály**

- Biztonsági szempontból kritikus funkciót lát el a termék
- Központi rendszerfunkciókat lát el a termék

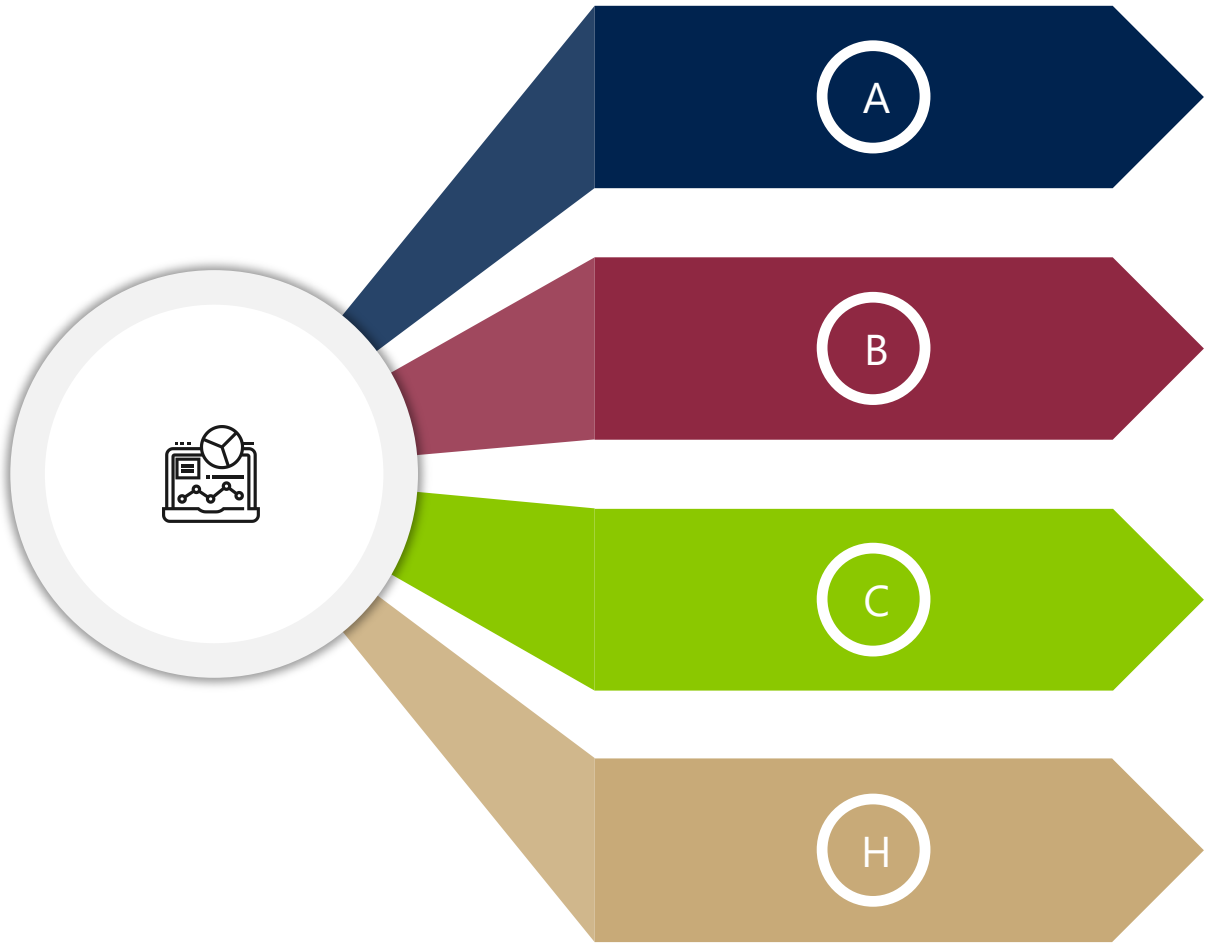
IIIa melléklet

Rendkívül kritikus termékek

Kritikus fontosságú termékek



Megfelelőségértékelés



Belső ellenőrzésen alapuló megfelelőségértékelési eljárás

EU-típusú vizsgálat

Belső gyártásellenőrzésen alapuló típusmegfelelőség

A teljeskörű minőségbiztosításon alapuló megfelelőség

Piacfelügyelet

Nemzeti kiberbiztonsági tanúsító hatóság

Nemzeti illetékes hatóság

Meglévő vagy új hatóság

Az (EU) 2019/1020 rendelettel összhangban nemzeti piacfelügyeleti hatóságok piacfelügyeletet végeznek az adott tagállam területén. A tagállamok meglévő és új hatóságot is kijelölhetnek piacfelügyeleti hatóságként eljáró hatóságnak, beleértve az (EU) 2022/2555 irányelv (NIS2) [8. cikk] cikkében említett nemzeti illetékes hatóságokat vagy az (EU) 2019/881 rendelet 58. cikkében említett kijelölt nemzeti kiberbiztonsági tanúsító hatóságokat...

Köszönöm a figyelmet!

SZTFH
Szabályozott Tevékenységek Felügyeleti Hatósága

MINDEN KIBERÜL

dr. Bencsik Balázs
kiberbiztonsag@sztfh.hu
Kiberbiztonsági Tanúsítási Igazgatóság