EURÓPAI UNIÓS KIBERBIZTONSÁGI ÜGYNÖKSÉG

MEGBÍZHATÓ ÉS KIBERBIZTONSÁGI SZEMPONTBÓL BIZTONSÁGOS EURÓPA

ENISA Stratégia

2020. június

MEGBÍZHATÓ ÉS KIBERBIZTONSÁGI SZEMPONTBÓL BIZTONSÁGOS EURÓPA

EURÓPAI UNIÓS KIBERBIZTONSÁGI ÜGYNÖKSÉG

ELŐSZÓ

Az ENISA – az Európai Uniós Kiberbiztonsági Ügynökség – több mint 15 éve kiemelt szerepet játszik abban, hogy megvalósuljon az Unió azon törekvése, hogy az uniós tagállamokkal, valamint az uniós intézményekkel és ügynökségekkel együtt Európa-szerte megerősítse a digitális bizalmat és biztonságot. A közösségek összefogásával az ENISA sikeresen hozzájárult Európa váratlan kiberbiztonsági eseményekre való felkészültségének és reagálási képességeinek megerősítéséhez.

Ezzel párhuzamosan gazdaságunk és társadalmunk digitalizációja drasztikus mértékben fokozódott, amint az a Covid19-válság során is megmutatkozott, amikor számos tevékenység folytatásához elengedhetetlenné vált a távoli informatikai megoldásokra való kollektív és tömeges áttérés. A válság rávilágított arra, hogy a számítógépes támadások elkövetői milyen mértékben használják ki az e technológiáktól való függőségünket. A krízis során egyértelművé vált az is, hogy a kiberfenyegetések a célzott támadások mellett immár kiterjednek a több millió vállalkozást és polgárt érintő tömeges fenyegetések új formáira is, beleértve a kifinomult zsarolóvírus-támadások növekvő számát. A digitális termékek és szolgáltatások gyors fejlődése – a számítási felhőtől és a videokonferenciától az 5G-ig és a mesterséges intelligenciáig – új kihívások feltárásának és kezelésének szükségességét is magával hozta.

Állandó megbízatásával, valamint megerősített feladataival és képességeivel az ENISA-nak minden eddiginél nagyobb szerepet kell játszania abban, hogy segítse az Uniót és tagállamait abban, hogy lépést tartsanak ezekkel a kihívásokkal, miközben Európa a kiberbiztonság új korszakának küszöbén áll.

Ennek érdekében az ENISA arra fog törekedni, hogy előre jelezze a releváns tendenciákat, továbbá mozgósítsa és megossza a legkorszerűbb szakértelmet és tudást mindenki számára. Támogatni fogja az Európai Bizottságot és a tagállamokat abban, hogy segítsék a köz- és magánszféra szereplőit és a polgárokat a kiberbiztonsági eseményekhez kapcsolódó kockázatok megelőzésében és kezelésében. A kiberbiztonsági tanúsítási keretrendszer megvalósításával az ENISA hozzá fog járulni a paradigmaváltáshoz azáltal, hogy javítja az Európában alkalmazott digitális megoldások biztonsági szintjét. Ezáltal mindenki számára javítani fogja a választás és a bizalom lehetőségét. Az Ügynökség emellett aktívan támogatni fogja az európai kiberbiztonsági operatív közösséget abban, hogy szorosan együttműködjön és felkészüljön arra, hogy közösen reagáljon az Európát érintő következő nagyszabású kiberbiztonsági esemény bekövetkeztekor.

Az ENISA új szerepének betöltésével a nyitottság, a gyorsaság és a megbízhatóság kulcsfontosságú szerepet játszik majd az ügynökség napi működésében, miközben szorosabban együttműködik a tagállamokkal és az Európai Bizottsággal a megközelítések összehangolása terén. Az ENISA arra is törekedni fog, hogy a jelenlegi klímaválsággal összefüggésben javítsa környezeti hatását és társadalmilag felelős és befogadó munkakörnyezetet teremtsen.

Ez a stratégiai dokumentum, amely az ENISA valamennyi munkatársának, igazgatótanácsi tagjainak és tanácsadó csoportjának bevonásával, együttműködésen alapuló és inkluzív folyamat során készült, meghatározza azokat az egyértelmű célkitűzéseket, amelyek az elkövetkező években meg fogják határozni az ENISA munkáját az előttünk álló számos kihívás kezelése érdekében.

Az igazgatótanács nevében

Jean-Baptiste Demaison
Az igazgatótanács elnöke

Krzysztof Silicki
Az igazgatótanács alelnöke

JÖVŐKÉP

Megbízható és kiberbiztonsági szempontból biztonságos Európa

KÜLDETÉS

Az Európai Uniós Kiberbiztonsági Ügynökség (EINSA) küldetése a tágabb közösséggel együttműködve az Unió-szerte egységesen magas szintű kiberbiztonság megvalósítása. Ennek érdekében kiberbiztonsági szakértői központként működik és független, magas színvonalú technikai tanácsokat és segítséget gyűjt és nyújt a tagállamoknak és az uniós szerveknek a kiberbiztonság területén. Hozzájárul az uniós kiberpolitikák kidolgozásához és végrehajtásához.

Célunk az összekapcsolt gazdaságba vetett bizalom megerősítése, az uniós infrastruktúra és szolgáltatások ellenálló-képességének és bizalmának fokozása, valamint társadalmunk és polgáraink digitális biztonságának megőrzése. Arra törekszünk, hogy az emberekre összpontosító, dinamikus, környezeti és társadalmi szempontból felelős szervezet legyünk.

ÉRTÉKEK

Közösségi megközelítés
Az ENISA közösségekkel dolgozik, tiszteletben tartva azok hatásköreit és szakértelmét, továbbá előmozdítja a szinergiákat és erősíti a bizalmat annak érdekében, hogy a lehető legjobban megvalósítsa küldetését.

Kiválóság
Az ENISA célja, hogy munkája során korszerű szakértelmet biztosítson, fenntartsa a legmagasabb szintű működési színvonalat és értékelje teljesítményét annak érdekében, hogy az innováció és az előrejelzés révén folyamatos fejlődésre törekedhessen.

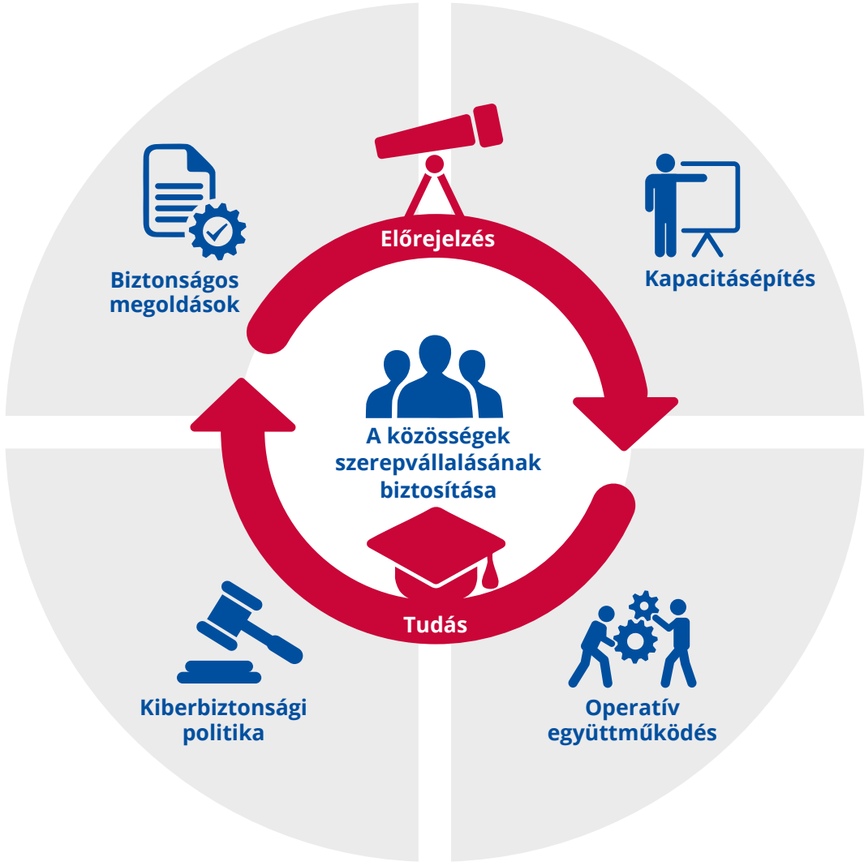
Feddhetetlenség/etika
Az ENISA szervezeti egységeiben és munkakörnyezetében tiszteletben tartja az etikai elveket és a vonatkozó uniós szabályokat és kötelezettségeket a méltányosság és az inkluzivitás biztosítása mellett.

Tisztelet
Az ENISA tiszteletben tartja a valamennyi szervezeti egységére és munkakörnyezetére kiterjedő alapvető európai jogokat és értékeket, valamint az érdekelt felek elvárásait.

Felelősség
Az ENISA felelősséget vállal, így biztosítja a szociális és környezetvédelmi szempontok integrálását a gyakorlatokba és eljárásokba.

Átláthatóság
Az ENISA nyílt, tényszerű és független eljárásokat, struktúrákat és folyamatokat alkalmaz, ezáltal korlátozza az elfogultságot, a félreérthetőséget, a csalást és a pontatlanságokat.

STRATÉGIAI CÉLKITŰZÉSEK



SO1

Stratégiai célkitűzés

A KÖZÖSSÉGEK SZEREPVÁLLALÁSÁNAK ÉS ELKÖTELEZETTSÉGÉNEK NÖVELÉSE A KIBERBIZTONSÁGI ÖKOSZISZTÉMA EGÉSZÉBEN

Háttér

A kiberbiztonság közös feladat. Európa egy ágazatokon átívelő, mindenre kiterjedő együttműködési keret létrehozására törekszik. Az ENISA kulcsszerepet játszik a tagállamok kiberbiztonsági szereplői, valamint az uniós intézmények és ügynökségek közötti aktív együttműködés ösztönzésében. Arra törekszik, hogy biztosítsa a közös erőfeszítések egymást kiegészítő jellegét azáltal, hogy hozzáadott értéket teremt az érdekelt felek számára, feltárja a szinergiákat és hatékonyan felhasználja a korlátozott kiberbiztonsági szakértelmet és erőforrásokat. A közösségek számára lehetőséget kell biztosítani, hogy magasabb szintre emeljék a kiberbiztonsági modellt.

Megvalósítandó céljaink

- A kiberbiztonsági koncepciókkal és gyakorlatokkal kapcsolatos, az egész Unióra kiterjedő legkorszerűbb tudásanyag létrehozása, amely együttműködést alakít ki a kiberbiztonság kulcsszereplői között, népszerűsíti a levont tanulságokat és az uniós szakértelmet és új szinergiákat hoz létre.
- Megerősített kiberökoszisztéma, amely magában foglalja a tagállami hatóságokat, az uniós intézményeket, ügynökségeket és szerveket, egyesületeket, kutatóközpontokat és egyetemeket, az ipart, a magánszektor szereplőit és a polgárokat, akik mind szerepet játszanak Európa kiberbiztonságának megteremtésében;

SO2

Stratégiai célkitűzés

A KIBERBIZTONSÁG MINT AZ UNIÓS SZAKPOLITIKÁK SZERVES RÉSZE

Háttér

A kiberbiztonság a digitális átalakulás sarokköve és arra minden ágazatban szükség van, ezért a szakpolitikai területek és kezdeményezések széles körében figyelembe kell venni. A kiberbiztonság nem korlátozódhat a technikai kiberszakértők szakmai közösségére. A kiberbiztonságot ezért valamennyi uniós szakpolitikai területbe be kell építeni. El kell kerülni a széttöredezettséget és egységes megközelítésre van szükség, ugyanakkor figyelembe kell venni az egyes ágazatok sajátosságait.

Megvalósítandó céljaink

- Olyan proaktív tanácsadás és támogatás valamennyi érintett uniós szintű szereplő számára, amely életképes és célzott technikai iránymutatások révén beépíti a kiberbiztonsági dimenziót a szakpolitikák kidolgozásának életciklusába;
- Kiberbiztonsági kockázatkezelési keretek, amelyeket minden ágazatban alkalmaznak, és amelyeket a kiberbiztonsági politika teljes életciklusa során követnek.

SO3

Stratégiai célkitűzés

HATÉKONY EGYÜTTMŰKÖDÉS AZ UNIÓN BELÜLI OPERATÍV SZEREPLŐK KÖZÖTT SÚLYOS KIBERBIZTONSÁGI ESEMÉNYEK ESETÉN

Háttér

Az európai digitális gazdaság és társadalom előnyei csak a kiberbiztonság szavatolásával valósulhatnak meg maradéktalanul. A kibertámadások nem ismernek határokat. A társadalom minden rétegét érinthetik, és az Uniónak készen kell állnia a tömeges (nagyméretű és határokon átnyúló) kibertámadásokra és kiberválságokra való reagálásra. A határokon átnyúló kölcsönös függőségek rávilágítottak arra, hogy a tagállamok és az uniós intézmények között hatékony együttműködésre van szükség a gyorsabb reagálás és az erőfeszítések valamennyi (stratégiai, operatív, műszaki és kommunikációs) szinten történő megfelelő összehangolása érdekében.

Megvalósítandó céljaink

- A tagállamok közötti, valamint az uniós intézményekkel folytatott együttműködés folyamatos, határokon és különböző szinteken átnyúló támogatása. Különösen az esetleges nagyszabású biztonsági eseményekre és válságokra tekintettel a kulcsfontosságú operatív szereplők közötti technikai operatív, politikai és stratégiai együttműködés erősítésének támogatása annak érdekében, hogy Unió-szerte lehetővé váljon az időben történő reagálás, az információmegosztás, a helyzetfelismerés és a válsághelyzetekkel kapcsolatos kommunikáció;
- A tagállamok kérésére átfogó és gyors technikai kezelés a váratlan biztonsági események és válságok kezelése során felmerülő technikai és operatív igények megkönnyítése érdekében.

SO4

Stratégiai célkitűzés

ÉLVONALBELI KOMPETENCIÁK ÉS KÉPESSÉGEK A KIBERBIZTONSÁG TERÉN AZ EGÉSZ UNIÓBAN

Háttér

A kibertámadások gyakorisága és kifinomultsága igen gyorsan növekszik, miközben az IKT-infrastruktúrák és -technológiák magánszemélyek, szervezetek és iparágak általi használata szintén gyorsan bővül. A kiberbiztonsági ismeretek és kompetenciák iránti igények meghaladják a kínálatot. Az Uniónak valamennyi szinten invesztálnia kell a kiberbiztonsági kompetenciák és kiváló képességek fejlesztésébe a nem szakértőktől a magasan képzett szakemberekig. A befektetéseknek nemcsak a kiberbiztonsági készségek fejlesztésére kell összpontosítaniuk a tagállamokban, hanem annak biztosítására is, hogy a különböző operatív közösségek rendelkezzenek a kiberfenyegetések kezeléséhez szükséges megfelelő kapacitással.

Megvalósítandó céljaink

- Összehangolt kiberbiztonsági kompetenciák, szakmai tapasztalat és oktatási struktúrák az Unióban a kiberbiztonsági ismeretek és kompetenciák iránti folyamatosan növekvő igények kielégítése érdekében;
- A kiberbiztonsággal kapcsolatos tudatosság és kompetenciák magas alapszintje az egész Unióban, a kiberbiztonság új tudományágakban való általános érvényesítése mellett;
- Megfelelően előkészített és tesztelt képességek, amelyek megfelelő kapacitással rendelkeznek a változó fenyegetettségi környezet kezelésére az Unióban.

SO5

Stratégiai célkitűzés

MAGAS SZINTŰ BIZALOM A BIZTONSÁGOS DIGITÁLIS MEGOLDÁSOK IRÁNT

Háttér

A digitális termékek és szolgáltatások nemcsak előnyökkel, hanem kockázatokkal is járnak, amelyeket azonosítani és enyhíteni kell. A digitális megoldások biztonságának értékelése és megbízhatóságuk biztosítása során alapvető fontosságú olyan közös megközelítés elfogadása, amelynek célja a társadalmi, piaci, gazdasági és kiberbiztonsági igények közötti egyensúly megteremtése. Egy átlátható módon működő, semleges szervezet növelni fogja a fogyasztók digitális megoldásokba és a tágabb digitális környezetbe vetett bizalmát.

Megvalósítandó céljaink

- Az Unió egész területén megvalósuló, kiberbiztonsági szempontból biztonságos digitális környezet, ahol a polgárok megbízhatnak az IKT-termékekben, -szolgáltatásokban és -folyamatokban azáltal, hogy tanúsítási rendszereket vezetnek be a kulcsfontosságú technológiai területeken;

SO6

Stratégiai célkitűzés

“

KIALAKULÓBAN
LÉVŐ ÉS A JÖVŐBELI
KIBERBIZTONSÁGI
KIHÍVÁSOK ELŐREJELZÉSE

Háttér

Az előrejelzési módszerek alkalmazása számos új, még gyerekcipőben járó vagy az általános alkalmazáshoz már közel álló technológia számára előnyös lenne. Az érdekelt felek, a döntéshozók és a szakpolitikai döntéshozók közötti párbeszédet lehetővé tevő strukturált folyamat révén korai mérséklési stratégiák kerülnének meghatározásra, amelyek javítják az Unió kiberbiztonsági fenyegetésekkel szembeni ellenálló-képességét és megoldásokkal szolgálnak a felmerülő kihívások kezelésére.

Megvalósítandó céljaink

- A kialakuló folyamatok és sémák megértése olyan előrejelzések és jövőbeli forgatókönyvek felhasználásával, amelyek hozzájárulnak az érdekelt felek előtt álló kiberkihívások enyhítéséhez;
- A felmerülő jövőbeli lehetőségek elfogadásából és az azokhoz való alkalmazkodásból eredő kihívások és kockázatok korai értékelése az érdekelt felekkel való együttműködés mellett a megfelelő mérséklési stratégiák kidolgozása során.

SO7

Stratégiai célkitűzés

HATÉKONY ÉS EREDMÉNYES KIBERBIZTONSÁGI INFORMÁCIÓ- ÉS TUDÁSMENEDZSMENT EURÓPÁBAN

Háttér

A kiberbiztonságot tápláló energia az információ és a tudás. Ahhoz, hogy a kiberbiztonsági szakemberek hatékonyan teljesíthessék célkitűzéseinket és folyamatosan változó környezetben dolgozhassanak – mind a digitális fejlődés, mind a szereplők tekintetében – annak érdekében, hogy szembenézhessenek korunk kihívásaival, a kiberbiztonsági információk és ismeretek összegyűjtésével, rendszerezésével, összegzésével, elemzésével, kommunikálásával és fenntartásával kapcsolatos állandó folyamatra van szükség. Minden szakasz alapvető fontosságú az információk és az ismeretek uniós kiberbiztonsági ökoszisztémán belül történő megosztása és kiterjesztése érdekében.

Megvalósítandó céljaink

- Megosztott információk és tudásmenedzsment az uniós kiberbiztonsági ökoszisztéma számára hozzáférhető, testreszabott, megfelelő időben történő és alkalmazható formában, megfelelő módszertannal, infrastruktúrákkal és eszközökkel, összekapcsolt és minőségbiztosítási módszerekkel a szolgáltatások folyamatos javítása érdekében.

AZ EINSA-RÓL

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az Unió azon ügynöksége, amelynek célja az Európa-szerte egységesen magas szintű kiberbiztonság megvalósítása. A 2004-ben létrehozott és az uniós kiberbiztonsági jogszabály által megerősített Európai Uniós Kiberbiztonsági Ügynökség hozzájárul az uniós kiberpolitikához, kiberbiztonsági tanúsítási rendszerek alkalmazásával javítja az IKT-termékek, -szolgáltatások és -folyamatok megbízhatóságát, együttműködik a tagállamokkal és az uniós szervekkel és segíti Európát abban, hogy felkészüljön a jövő kiberbizotnsággal kapcsolatos kihívásaira. A tudásmegosztás, a kapacitásépítés és a figyelemfelkeltés révén az Ügynökség a legfontosabb érdekelt felekkel együtt arra törekszik, hogy megerősítse az összekapcsolt gazdaságba vetett bizalmat, fokozza az uniós infrastruktúra ellenálló-képességét és végső soron megőrizze Európa társadalmának és polgárainak digitális biztonságát. Az ENISA-ról és munkájáról további információkat találhat a www.enisa.europa.eu weboldalon.

TP-02-20-759-HU-N

ENISA
Európai Uniós Kiberbiztonsági Ügynökség

Athéni iroda
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Görögország

Irákliói iroda
95 Nikolaou Plastira
700 13 Vassilika Vouton, Iráklio, Görögország

enisa.europa.eu