PROJEKT EREDMÉNYEIT BEMUTATÓ KIADVÁNY

KÖFOP-2.2.2-VEKOP-16-2016-00001.

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE

Tartalomjegyzék

Bevezető

Az Internet felől érkező támadások, fenyegetések felismerése és azok megelőző elhárítása egyre nagyobb kihívás elé állítja az ebben érdekelt civil és kormányzati szervezeteket, ügynökségeket, amelyek tevékenységük során folyamatosan szembesülnek a napról-napra fejlődő eljárásokkal, módszerekkel, valamint a permanensen növekvő adatmennyiségekkel.

A korábban alkalmazott eljárások a felgyorsult világban már nem, vagy csak korlátozottan alkalmazhatóak, figyelemmel arra, hogy az információ mennyisége már meghaladja a jelenlegi filozófia szerint belátható időn belül feldolgozható mértéket, ezzel összefüggésben új erőforrásokra, egyre több és egyre mélyebb ismeretekkel rendelkező szakemberekre van szükség.

Az információ teljes, vagy részleges gépi feldolgozása jelentősen támogatja a kibervédelemben érintett szervezeteket és az általuk végzett ez irányú tevékenységet azáltal, hogy biztosítja a nagy mennyiségű információból a releváns információk felismerését, kiválasztását, ezáltal a szükséges döntések előkészítését, meghozatalát. Ennek eredményeként lehetőség nyílik, hogy a jól képzett szakemberek képességei a konkrét elhárító, eseménykezelő, illetve tudatosító tevékenységekre legyen felhasználható.

A Nemzetbiztonsági Szakszolgálat KÖFOP-2.2.2-VEKOP-16-2016-00001 kódszámú, „KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése” elnevezésű projektje keretében megvalósított fejlesztéssel láthatóvá, illetve felderíthetővé válnak egyes, a Közigazgatás- és Közszolgáltatás-fejlesztés Operatív Program keretében végrehajtott fejlesztések eredményeként létrehozott közszolgáltatások, valamint korrupciónak kitett rendszerek kapcsán esetlegesen bekövetkező korrupciós cselekmények (pl. adatszivárogtatás) és egyéb visszaélések (pl. hálózati betörési kísérlet, adatlopás, weboldal rongálás). A megvalósított fejlesztésekkel összefüggésben megjelenő IT alapú módszerek feltárása és visszacsatolása nagyban hozzájárulhat a közigazgatási szervek átláthatóságának növeléséhez, az integritás erősítéséhez, valamint a Szabályozott Elektronikus Ügyintézési Szolgáltatásokba és biztonságos adatkezelésbe vetett közbizalom erősítéséhez.

A projekt keretében megvalósított fejlesztés a Nemzeti Korrupcióellenes Programmal összhangban preventív (megelőző) passzív eszközökkel jelentősen hozzájárul a korrupció elleni eredményes fellépéshez azáltal, hogy a nemzeti adatvagyont, illetve az állampolgárok személyes adatait kezelő rendszerek észlelési képességének javításával, valamint korrupciós szempontból érzékeny rendszerek biztonságának erősítésével javítja a közigazgatás intézményeinek működésébe, elektronikus adatok kezelésébe vetett közbizalmat.

A KÖFOP-2.2.2-VEKOP-16-2016-00001. projekt alapadatai

Kedvezményezett: Nemzetbiztonsági Szakszolgálat

Projekt címe: KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése

Támogatás összege: 2 500 000 000 Ft

Támogatás mértéke: 100 %

Projekt bemutatása: A projekt célja a korrupciós kockázatnak kitett közigazgatási információs rendszerek védelmének megerősítése, olyan korai figyelmeztető rendszer kialakítása, amellyel láthatóvá, illetve felderíthetővé válnak az esetlegesen bekövetkező korrupciós cselekmények és egyéb visszaélések

Projekt időtartama: 2016.02.16. – 2022.03.31.

Projektazonosító: KÖFOP-2.2.2-VEKOP-16-2016-00001.

A kedvezményezett bemutatása

Nemzetbiztonsági Szakszolgálat

25 évvel ezelőtt, 1996. március 27-én, egy modern és előremutató kormányzati döntés alapján került megalapításra a Nemzetbiztonsági Szakszolgálat (NBSZ). A konszenzusos politikai elhatározás értelmében a titkosszolgálati eszközök alkalmazása egy különálló, a titkos információgyűjtésre feljogosított szervezetektől független, ilyenformán elfogulatlan intézményhez került kiszervezésre. Az NBSZ létrehozása megfelelt a rendszerváltáskor megfogalmazódott társadalmi-politikai elvárásoknak – kiemelten a jogállamiság kritériumai, a magánélet és a személyes adatok védelméhez fűződő jogok érvényesítése –, miközben gazdasági szempontból is jelentős előnyöket hordozott magában, és a profiltisztítás eredményeként valamennyi érintett szereplő esetében növelte a hatékonyságot.

Szolgáltatásai kezdetben gyakorlatilag a titkos információszerzés területére koncentrálódtak, de az elmúlt 25 év során ezek tartalma bővült, illetve a spektruma a társadalmi elvárásoknak megfelelően és a technológiai fejlődést lekövetve folyamatosan szélesedett, így mára – miközben a titkos információszerzés terén megkerülhetetlen közreműködővé vált – jelentős szerepet tölt be az elektronikus információ- és kiberbiztonsági szervezetrendszerben is.

A fejlődés alapvető törvényszerűségeire figyelemmel egyre gyakoribb, hogy új, kihívásokat tartogató feladatok ellátására kerül felhatalmazásra az NBSZ, ahol a teljesítmény színvonalát a képességek palettája és minősége határozza meg. Az információs és kommunikációs technológiák forradalmának korában elengedhetetlen, hogy az NBSZ valamennyi szolgáltatási területén folyamatosan kutassa, ismerje és magabiztosan használni is képes legyen a megjelenő új technikai módszereket és eljárásokat, amelyek napi rutinba történő illesztése újszerű gondolkodást, proaktivitást követel meg.

Az elmúlt évtizedben az NBSZ működési környezetét a minden korábbinál intenzívebb technikai fejlődés jellemezte, és – amennyiben továbbra is meg kívánt felelni alapvető rendeltetésének, avagy a széles értelemben vett biztonság garantálásának – nem lehetett opció a technológiai trendek figyelmen kívül hagyása: a tegnap még sci-fi-nek tűnő fejlesztésekre módszertani és technológiai innovációval kellett válaszolnia.

Hazai kibervédelem helyzete

Hazánkban már nagyon korán felismerték a szakemberek az információbiztonság fontosságát, így az első szabályzó már 1994-ben napvilágot látott. Ez volt a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának 8. sz. ajánlása, egy informatikai biztonsági módszertani kézikönyv, amely egy tájékoztató volt az informatikai biztonság megteremtésének legfontosabb elemeiről. Ennek célja az volt, hogy a szervezetek felkészülhessenek az informatikai biztonsági koncepciójának kialakítására. A kézikönyv tartalmazott egy kockázatelemzési módszertant is.1996-ban jelent meg a MeH ITB 12. sz. ajánlása, amely az informatikai rendszerek biztonsági követelményeit tartalmazta. Ez nem csak logikai védelem előírásait jelentette, hanem részletes követelményeket és védelmi intézkedéseket is az informatikai biztonság adminisztratív és a fizikai védelem területeire, valamint a szervezeti, személyi és fizikai biztonság kérdéseire is. Sajnos azonban ezeket az elveket –néhány kivételtől eltekintve -nem sikerült a gyakorlatban megvalósítani, ugyanis az ajánlásokat nem tették kötelezővé.

2013-ban a fentebb tárgyaltak szerint megalakult a magyar kiberbiztonsági szervezetrendszer, amelynek felülvizsgálata során 2015-ben létrejött a Nemzeti Kibervédelmi Intézet.

A Nemzeti Kibervédelmi Intézeten kívül a honvédelmi ágazat elektronikus információs rendszereinek eseménykezelési, hatósági-felügyeleti és sérülékenységvizsgálati feladatainak ellátása érdekében Kibervédelmi Központ működik a Katonai Nemzetbiztonsági Szolgálat szervezetén belül. Ezen túl a Honvédség szervezetén belül Kibervédelmi Szemlélőség is működik.

A világ országaiban számtalan módon működnek kibervédelmi szervezetek. A magyar kibervédelmi szervezetrendszer – hasonlóan az amerikai, a brit és a német példához – hivatásos szerveknél, titkosszolgálatoknál került elhelyezésre.

Magyarország elkötelezettségét a téma iránt, mi sem bizonyítja jobban, hogy hazánk a 19. helyen végzett a Nemzetközi Távközlési Egyesület (ITU) Globális Kiberbiztonsági Felmérésén (Global Cybersecurity Index- GCI). Az ENSZ infokommunikációs technológiával foglalkozó ügynöksége 2013 óta minden évben – objektív metodikát alkalmazva – felméri az államok kiberbiztonsággal kapcsolatos érettségét és elkötelezettségét. A kiberbiztonság, mint téma, széles alkalmazási területként értelmezhető, ezért az online felmérés is több iparágat, szektort ölelt fel. Az egyes országok fejlesztési vagy szerepvállalási szintjei öt főpillér (jogi, technikai, szervezeti, kapacitásbővítési és együttműködés intézkedések) mentén kerültek értékelésre, majd ezen részeredményeket összesítve alakult ki az összesített pontszám. A legutóbbi felmérésen Magyarország – regionális szinten – a 19., míg az ITU 195 tagállama közül az 31. helyen végzett. A korábbi évekhez képest az eredmény jelentős előrelépésnek tekinthető.

Nemzeti Kibervédelmi Intézet

Az Országgyűlés 2013-ban – figyelembe véve Magyarország Biztonsági Stratégiáját, Magyarország Nemzeti Kiberbiztonsági Stratégiáját, valamint ez utóbbit is megalapozó Európai Unió kiberbiztonsági stratégiáját – megalkotta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt (Ibtv.), amely 2013. július 01-jén lépett hatályba. Az Ibtv. célként fogalmazza meg a nemzeti elektronikus adatvagyon, valamint az állami- és önkormányzati szervek elektronikus információs rendszereinek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonságának erősítését; deklarálja, hogy az elektronikus információs rendszerek biztonságáért az üzemeltető, működtető állami szerv a felelős.

A törvény továbbá létrehozta a hazai kibervédelmi szervezetrendszert, amelynek alapvető rendeltetése, hogy az állami szervek információbiztonsági feladatainak végrehajtását biztonsági szolgáltatásokkal támogassa, ellenőrizze, az állami szervezetrendszer egésze tekintetében a biztonságtudatosságot fejlessze. A szervezetrendszer stratégiai szintű eleme a Nemzeti Kiberkoordinációs Tanács, amelynek feladata a stratégia kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése, valamint a magánszféra szakmai véleményének kormányzati döntéshozatalba történő becsatornázására létrehozott Kiberbiztonsági Fórum.

A szervezetrendszer operatív elemei:

- a jogszabályi előírások ellenőrzésével és érvényesítésével foglalkozó információbiztonsági hatóság,
- a kibertérből érkező támadásokkal és fenyegetettségekkel közvetlenül foglalkozó eseménykezelő központ, valamint
- az informatikai rendszerek gyenge pontjainak feltárását, a rendszer védelmi képességek tesztelését (sérülékenységvizsgálat) végző szerv.

Az Ibtv. 2015. évi módosítása eredményeként az állami és önkormányzati szervezetek információs rendszerei tekintetében a fenti operatív feladatok működtetésére az NBSZ került kijelölésre, amelynek szervezetén belül 2015. október 1-jével létrehozásra került a Nemzeti Kibervédelmi Intézetet (NKI).

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) a 2019. január 1-jén hatályba lépett jogszabály-módosítások eredményeként ellátja

- az eseménykezelési feladatokat a létfontosságú információs rendszerek és rendszerelemek, valamint
- az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben meghatározott bejelentés-köteles szolgáltatást – úgymint online piactér, internetes keresőszolgáltatás, valamint felhőszolgáltatás – nyújtó szolgáltatók esetében az eseménykezelési, valamint a hatósági felügyeletet.

Az NBSZ NKI jogszabályi feladatai közé tartozik továbbá az ún. „nemzeti kapcsolattartó pont” működtetése, amelynek feladata az Európai Unión belüli nagy hatású kiber-incidensek hazai koordinálása, az incidensekkel kapcsolatos jelentések fogadása, küldése a nemzetközi partner-szervezetek irányába.

A Nemzeti Kibervédelmi Intézet főbb szolgáltatásai

Incidenskezelés

Az NBSZ NKI rendeltetése az informatikai rendszerek informatikai biztonsági támogatása országosan, amely egyrészt megelőző jellegű, a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követésére és az IT rendszereket üzemeltetők részére történő kommunikálására (sérülékenység-menedzsment), másrészt pedig reaktív jellegű, a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és a kezelésük koordinációjára irányul. Az NBSZ NKI nem ellenőrzi az internet-felhasználást, és nem tilt le semmilyen honlaphoz való hozzáférést, csupán figyelmeztet a veszélyes helyekre.

A sérülékenység-menedzsment során az NBSZ NKI információkat gyűjt a szoftver-sérülékenységekről és káros szoftverekről, megvizsgálják azok ügyfélkörre vonatkozó relevanciáját, és általános körben vagy célzottan tájékoztatják a fenyegetés kiváltotta biztonsági esemény megelőzése érdekében ezen rendszereket üzemeltetőket.

Az incidenskezelési tevékenység során folyamatosan fogadja az IT rendszereket érő incidensek bejelentéseit, és megteszi az alapvető intézkedéseket (incidensek nyilvántartásba vétele, bejelentő visszatájékoztatása, alapvető információk azonosítása, stb.). A bejelentett incidens felszámolása során a következő lépés a jogosultsággal és/vagy képességgel rendelkező szerv/személy tájékoztatása a teendőkről, szükség esetén kapcsolattartás a bejelentővel, valamint az érintett incidens felszámolásának nyomon követése (incidens-koordináció).

Amennyiben szükséges, az incidensre utaló jelek alapján összegyűjti az incidens felderítéséhez szükséges információkat (pl.: naplóadatok) és ezek elemzésével megkísérlik rekonstruálni az incidens kiváltó okait, egyúttal javaslatot tesz a hasonló incidensek megelőzését vagy az okozott kár enyhítését támogató informatikai védelmi intézkedésekre.

Ellátott feladatok:

- biztonsági események kezelése;
- fenyegetésmenedzsment;
- ügyeleti szolgálat;
- elemzés/értékelés;
- kibervédelmi gyakorlatokon való részvétel, gyakorlatok szervezése;
- képzés, tudatosítás;
- információvédelmi felelősök kijelölésének támogatása;
- biztonságiesemény-kezelés kapcsán együttműködés a központi szolgáltatóval (NISZ Zrt.) és az ügyfelekkel;
- rendszeres vezetői tájékoztatás, negyedéves jelentések készítése.

Az NBSZ NKI egyik kiemelt feladata a biztonságtudatosság növelése a felhasználók vonatkozásában. A kibervédelem legolcsóbb és leghatékonyabb módja a biztonságtudatos használat. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne a megfelelő szinten kialakítható. A tudatosítás számos

formában megjelenhet, mint például szakmai anyagok és útmutatók készítése, közvetlenül kifejtett oktatási vagy képzési tevékenység, a kiberbiztonság hangsúlyának növelése a médiában.

A tudatosító tevékenység számos réteget céloz, ezek közt elsősorban kell említeni a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését, és tőlük várható el a védelmi intézkedések működtetése), és a felhasználókat, akiket meg kell tanítani az internet és az információs technológiák biztonságos használatára, saját és a rájuk bízott adatok felelős és szakszerű kezelésére.

Hatósági tevékenység

A hatóság az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. Amennyiben a szervezet a hatósággal nem működik együtt, úgy – költségvetési szerv esetében – a hatóságnak joga van kirendelni ún. információbiztonsági felügyelőt, indokolt, súlyosabb esetben akár öt millió forintos bírság kiszabására is lehetősége van.

A hatóság ellenőrző funkciója erőteljes támogató funkcióval is bír, ugyanis jogosult a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában véleményezni és ellenőrizni az információbiztonsági követelmények megtartását. Az információtechnológiai fejlesztések elektronikus információbiztonsága szempontjából kiemelt fontosságú, hogy a vonatkozó előírások a rendszerek teljes életciklusa alatt következetesen és maradéktalanul megvalósításra kerüljenek és a fejlesztések eredményeként önmagukban is teljes, továbbá a meglévő rendszerekhez funkcionálisan és biztonsági aspektusból is harmonikusan és költséghatékonyan illeszkedő rendszerelemek, rendszerek épüljenek ki.

A hatóság feladatai:

- nyilvántartások vezetése;
- engedélyezések/hozzájárulások;
- Európai Gazdasági Térség (EGT) tagállamaiban történő elektronikus információs rendszer üzemeltetés tekintetében engedélyezési eljárás lefolytatása;
- kötelezések-a feltárt hiányosságok pótlásának elrendelése, ellenőrzése;
- szankcionálások:
    - felszólítás;
    - bírság;
    - információbiztonsági felügyelő kirendelésének kezdeményezése;
- helyszíni ellenőrzés éves ellenőrzési terv alapján (fizikai, logikai);
- beküldött iratok alapján történő hivatali ellenőrzés (adminisztratív);
- a fejlesztési projektek tervezési szakaszában ellenőrizni az információbiztonsági követelmények megtartását;
- kockázatelemzés.

Sérülékenységvizsgálat

A sérülékenységvizsgálat célja az esetleges biztonsági események bekövetkeztét megelőzően az elektronikus információs rendszer gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása. A sérülékenységvizsgálat végrehajtása során a vizsgálat alá vont elektronikus információs rendszerben az NBSZ NKI munkatársai felkutatják többek között a potenciális szoftverhibákat, gyenge jelszavakat, hibás beállításokat, amelyeket egy támadó képes lenne kihasználni, és ezeken keresztül kárt okozni a rendszerben. A sérülékenységvizsgálat eredményeként előálló vizsgálati jelentésben (állásfoglalás) a szakértők minden esetben javaslatot tesznek az azonosított sérülékenységek kijavítására is.

A vizsgálat lehet:

- külső (az internet irányából feltérképezhető információk összegyűjtése);
- belső (a szervezet hálózatának, informatikai eszközének vizsgálata);
- webes (az szervezet nyílt, vagy korlátozott elérésű webes rendszerének vizsgálata);
- vezeték nélküli hálózat (a vezeték nélküli hálózatának (WLAN) biztonsági vizsgálata);
- automatizált (automatizált eszközökkel, rendszeres időközönként végzett szoftveres sérülékenységvizsgálat a szervezet internet irányából elérhető rendszereire);
- pszichológiai manipulációs (a munkatársak hiszékenységét kihasználó információszerzés).

Biztonságirányítás

Míg az NBSZ NKI egyes szakterületei kívülről támogatják az érintett szerveket abban, hogy saját rendszereik védelmét ellássák, és ennek keretében kialakítsák saját ún. információbiztonsági irányítási rendszerüket (röviden: biztonságirányítási rendszer), addig a biztonságirányítási szakterület ezt a feladatot, az NBSZ számára kijelölt kormányzati rendszerek esetében, az informatikai biztonsági feladatok vonatkozásában, tevőlegesen főtevékenységeként végzi. A szakterület főtevékenysége mellett szakmai támogatást biztosít a többi szakterület számára.

KÖFOP-2.2.2-VEKOP-16-2016-00001. sz. projekt bemutatása

A Projekt indokoltsága, célja

A Kormány által 2014-2020 időszak vonatkozásában elfogadott Közigazgatás- és Közszolgáltatás Fejlesztési Stratégiában (KKFS) megfogalmazott cél, hogy a magyar közigazgatás szervezetten, következetes és átlátható intézményi struktúrában, korszerű és ügyfélbarát eljárásrenddel, költséghatékonyan, rövid ügyintézési határidőkkel működjön. Kiemelt célként támasztotta a közigazgatással szemben a Kormány az intézmények modern szervezeti keretek közt történő működtetését, a közigazgatási dolgozók szakmai felkészültségét és nemzeti hivatástudattal történő professzionális feladat végrehajtását, valamint a közigazgatási folyamatok gazdaságosságát és rugalmasságát.

Az állampolgárok olyan stabil és biztonságos informatikai háttérrel történő támogatást várnak el az államtól, amely lehetővé teszi a közigazgatás belső folyamatainak, illetve a lakosságot és vállalkozásokat célzó közigazgatási szolgáltatások nagyarányú elektronizálását, továbbá az állami érdekkörbe tartozó információk és tartalmak széles körű digitalizációját és nyilvános hozzáférhetővé tételét.

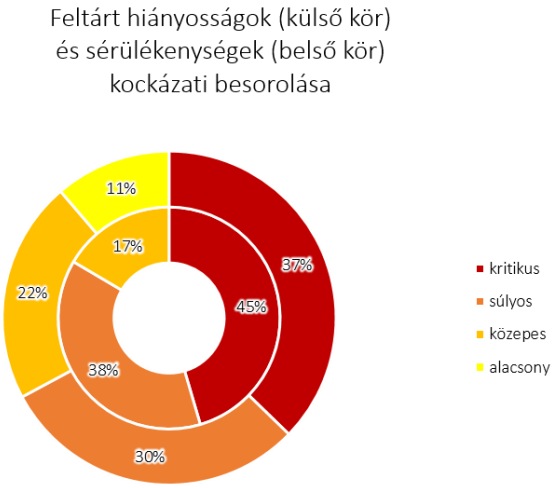
Ezen célok mentén az NBSZ fejlesztése hozzájárul a fenti célkitűzések eléréséhez azáltal, hogy a projekt eredményeként a közigazgatási folyamatok átláthatóságának növelését szolgáló, korrupciós kockázatokat csökkentő észlelési képesség, valamint egyes magas korrupciós védelmi rendszer került kifejlesztésre. A biztonságtudatosság erősítését, a kompetenciafejlesztést célzó képzések és az IT biztonságra irányuló szemléletformálás emellett támogatja az emberi erőforrás fejlesztését, közvetett hatásként pedig az etikus működés megerősítését a közszolgálatban.

A projekt Kormányzati elvárásokhoz, valamint az Operatív Programhoz történő illeszkedését az adja, hogy a KÖFOP keretében megvalósuló, nemzeti szinten kiemelten fontos IT fejlesztések, valamint korrupcióval fenyegetett kiemelten fontos rendszerek biztonsága, ezáltal a magyar közigazgatás integritása, valamint korrupciós ellenállóképessége erősítésre kerül. Ezen cél eléréséhez rendkívüli fontossággal bír annak szükségessége, hogy az egyes IT rendszerek üzemeltetői számára valós idejű adatok álljanak rendelkezésre ezen rendszereket érő esetleges támadásokról és normálistól eltérő hálózati forgalmi anomáliákról. Az IT biztonság megteremtésével – a Kormányzat elvárásával összhangban – a védett rendszerek, közigazgatási folyamatok átláthatósága és integritása jelentősen javulhat.

A Projekt eredményei

EMIR[1] és FAIR[2] rendszerek IT biztonságának megerősítése

Az NBSZ 2015 elején kezdte meg nevezett rendszerek kapcsán az IT biztonsági szolgáltatásnyújtás előkészületeit, melynek első lépése a rendszerek aktuális biztonsági állapotának felmérése volt. Ennek keretében információbiztonsági audit és sérülékenységvizsgálat került lefolytatásra. Mindkét vizsgálat nagyszámú biztonsági kockázatot tárt fel, amelyek veszélyeztették a rendszerek által nyújtott szolgáltatásokat és az abban kezelt adatok biztonságát. A hiányosságok és kockázatok elsősorban a biztonsági folyamatok hiányosságaira és a felügyeleti képesség gyengeségeire voltak visszavezethetőek.



A projekt keretében megvalósított fejlesztések (biztonsági eseménykezelő rendszer létrehozása, informatikai biztonsági infrastruktúra megerősítése, informatikai biztonsági irányító rendszer és biztonsági irányító központ kialakítása) az EMIR és FAIR rendszerek informatikai biztonsági feladatainak ellátását segítik azáltal, hogy biztosítják az informatikai biztonsági infrastruktúrákat és az elérésükhöz szükséges biztonsági irányító központot. A rendszerek biztonsági üzemeltetését, a szükséges biztonsági eseménykezelési megbízottakat, auditort és az operátori, jogosultságkezelői feladatok ellátását a rendszereken keresztül az NBSZ biztosítja.

A projekt keretében megerősítésre került a magas korrupciós kockázati index-szel bíró rendszerek (EMIR és FAIR) biztonsága, ami egyrészt biztosítja e rendszerek védelmének jogszabályi megfelelőségét, másrészt csökkenti a visszaélés kockázatát.

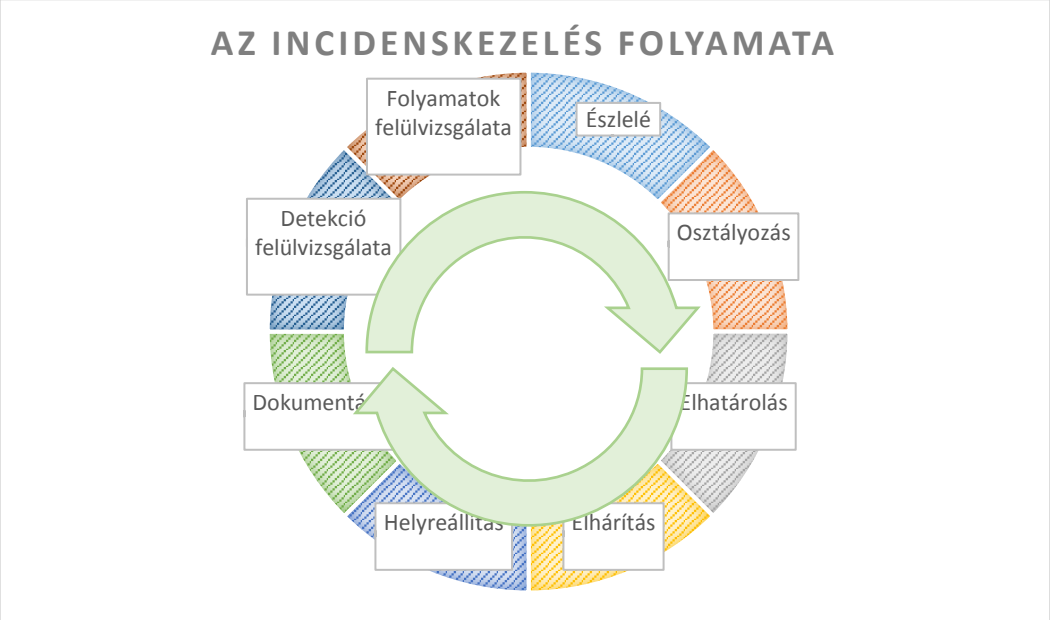
Az EMIR és FAIR biztonságfelügyeleti szolgáltatása horizontálisan bővíthető: a szolgáltatás oly módon került kialakításra, hogy adott esetben – a rendszerek illesztéséhez szükséges beruházásokat követően – további rendszerek kapcsolhatóak be e felügyeleti szolgáltatásba.

Az EMIR és FAIR rendszerek esetében a Biztonságirányítási szakterület SOC szolgáltatást nyújt, melynek legfőbb tevékenységei a felügyelt rendszerek loggyűjtése és logelemzése, amelynek keretében SIEM rendszerbe, egy központi adatbázisba integrálja és feldolgozza a SOC csapat által felügyelt rendszerek eseménynaplóit. Az események feldolgozása után, előre definiált szabályok alapján a bekövetkezett offense-ek vizsgálata történik. Az incidensek vizsgálata során, a védett rendszerek

[1] Egységes Monitoring és Információs Rendszer

[2] Fejlesztéspolitikai Adatbázis és Információs Rendszer

felhasználói vagy vezetői által bejelentett események kivizsgálása történik. Szükséges az eszkaláció megállítása, amely arra irányul, hogy megakadályozza az esemény továbbterjedését. Az incidens kezelés során -amennyiben szükséges- a SOC javaslatot tesz az incidens elhárítására, szakmai szempontok alapján támogatja az elhárítási folyamatot. A SOC -az incidens súlyosságától függően- elvégzi az incidensek kiváltó okainak utólagos elemzését, az újbóli bekövetkezés kockázatának csökkentése érdekében. Amennyiben hiányosságot tár fel, akkor új információvédelmi eljárások, rezsim intézkedések bevezetését és implementálását támogatja. Új védelmi koncepciók vizsgálatát, azok kidolgozását, meglévő rendszerek véleményezését végzi, továbbá időszakos jelentéseket készít a felügyelt rendszerekről. A szakterület új sérülékenységpublikációk megjelenését keresi és elemzi, érintettség megállapítást végez a védett rendszerek esetében. Valós fenyegetés esetén a felügyelt rendszerek információbiztonsági vezetőjét azonnal értesíti, védekezési intézkedéseket dolgoz ki a fenyegetés kezelésére.



Az incidenskezelési tevékenység során a SOC folyamatosan fogadja az IT rendszereket érő incidensek bejelentéseit és megteszi az alapvető intézkedéseket (incidensek nyilvántartásba vétele, bejelentő visszatájékoztatása, alapvető információk azonosítása stb.). A bejelentett incidens felszámolása során a következő lépés a jogosultsággal és/vagy képességgel rendelkező szerv/személy tájékoztatása a teendőkről, szükség esetén kapcsolattartás a bejelentővel, valamint az érintett incidens felszámolásának nyomon követése (incidens-koordináció). Amennyiben szükséges, az incidensre utaló jelek alapján összegyűjti az incidens felderítéséhez szükséges információkat (pl.: naplóadatok, egyéb állományok) és ezek elemzésével megkísérli rekonstruálni az incidens kiváltó okait, egyúttal javaslatot tesz a hasonló incidensek megelőzését vagy az okozott kár enyhítését támogató informatikai védelmi intézkedésekre, képzésekre.

A szolgáltatás bővítésére vertikális lehetőség is van: további szakértők bevonásával a biztonsági folyamatok megerősíthetőek, illetve a jelenleg el nem látott biztonsági funkciók is elláthatóak (pl. erőteljesebb részvétel a rendszerek fejlesztésében és az újonnan létrehozott szoftver verziók tesztelésében).

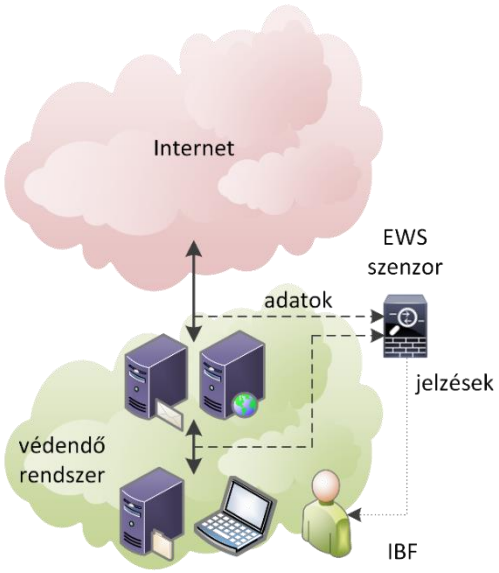
Igény esetén, a humán és technológiai feltételek megteremtésével közép-hosszú távon az NBSZ NKI akár szélesebb ügyfélkör számára is biztosíthat biztonságfelügyeleti és biztonságirányítási szolgáltatásokat, kiegészítve a jelenleg is széles szolgáltatási portfolióját (hatósági feladatok, eseménykezelés, fenyegetéselemzés, sérülékenységvizsgálat, tanácsadás, stb.).

Korai Figyelmezetető Rendszer megvalósítása, EWS (Early Warning System) szolgáltatás bevezetése

A KÖFOP projektek keretében, igazodva a kormányzati stratégiákhoz számos elektronikus közszolgáltatás ki- illetve továbbfejlesztése valósult meg, amely indokolttá tette a KÖFOP-os rendszerek információbiztonsági sebezhetőségét, illetve a rendszerek által kezelt nemzeti adatvagyon - 2012. évi C tv. XXV. fejezet 265. § (1), 422. § (1) d) 422. § (1) bek. d), 423. § (1) bek. 424. § (1) a) – ellen elkövetett bűncselekmények és felmerülő korrupciós fenyegetettségeket csökkentő folyamatok és rendszerek kialakítását, ezáltal növelve az érintett szervezetek integritását.

A kormányzati IT rendszerek üzemeltetői esetenként elégtelenül, vagy csak részlegesen rendelkeznek eszközrendszerrel (és kellő kompetenciával) az Internetről irányuló támadások észleléséhez, azonosításához és elemzéséhez. A szakemberek esetenként ellenérdekeltséget vélnek az informatikai biztonsági események törvényszerű bejelentésében, és így a biztonsági események – akár az észlelés hiánya, akár a bejelentés elmaradása miatt – nem, vagy késedelmesen válnak ismertté az NBSZ NKI számára. Emiatt az NBSZ NKI nem képes támogatni az incidensek kivizsgálását és elhárítását, valamint figyelmeztetni az esetleges további érintetteket.

Központi észlelési képesség és az ebből származó információk hiánya miatt nem volt átfogó, valós idejű kép a kormányzati hálózatok, rendszerek biztonsági helyzetéről.



Az NBSZ projektje keretében kialakításra került az EWS rendszer, amely az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának ún. szenzorokkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményeket (IDS funkcionalitás). Az EWS jelzéseket, adatokat és ezekre épülő szolgáltatásokat nyújt az egyes védendő rendszerekre vonatkozóan azok fenntartó intézményeinek kijelölt munkatársai és az NBSZ NKI számára.

Az EWS egyedülálló előnye, hogy a csatlakozó szereplőknek egységesen magas szintű kiegészítő védelmet nyújt és annak kihasználáshoz szükséges oktatást biztosít – mindezt megbízható kormányzati partnertől, központi finanszírozással.

Az EWS segítségével az intézmény számára hamarabb és nagyobb mértékben válhatnak láthatóvá, illetve ezáltal kezelhetővé a rendszert érintő támadások (pl. hálózati betörési kísérlet, adatlopás, weboldal rongálás), visszaélések, korrupciós cselekmények (pl. adatszivárogtatás, zsarolási kísérlet) és kockázatok (pl. sérülékeny vagy illetéktelen eszközök és szolgáltatások, lappangó kártevők).

Az EWS csatlakozással az intézményeknek csökkennek az incidens kivizsgáláshoz kapcsolódó adminisztratív terhei, mivel a tipikusan átadandó adatok egy része már eleve elektronikus formában az NBSZ NKI rendelkezésére áll, valamint az NBSZ NKI ezen adatok előzetes elemzésével és a védendő rendszer felépítésének ismeretében célzottabb javaslatot tud tenni a még szükséges műszaki adatok begyűjtésére illetve az indokolt védelmi intézkedésekre vonatkozóan.

A fejlesztés eredményeként az értesítési idő[3] a korábban átlagosan mért 104 óráról másodpercekre csökkent, amely elősegíti, hogy a közigazgatás EWS-be bevont szervezetei, rendszerei biztonságosabb és stabilabb környezetben működjenek (elsősorban külső – kiber-támadásoktól). Ennek eredményeképpen az újonnan kialakított EWS rendszer számos további rendszer biztonságosabb működéséhez járul hozzá.

A projekt megvalósításával az EWS rendszerbe jelenleg 26 szervezet, szervezeti egység került bevonásra, az EWS szolgáltatás 60 rendszerre került kiterjesztésre, amelyek 22 KÖFOP projekt keretében kerültek megvalósításra.

Az EWS központi tároló rendszer moduláris kiépítése révén, hosszú távon képes kiszolgálni az időközben felmerülő megnövekedett igényeket, ebből következően időtálló, fejleszthető infrastruktúrát képez. A megoldás a későbbiekben, addicionális komponensek, illetve licencek segítségével mind horizontálisan, mind vertikálisan egyaránt bővíthető, így a későbbiekben bevonásra kerülő védendő rendszerek adatainak tárolási feltételei továbbfejlesztéssel biztosíthatóak.

[3] Értesítési idő a közigazgatási szervezetek elektronikus rendszereit érintő hálózati forgalomelemzéssel azonosítható biztonsági esemény (2013. évi L. tv. 1. § (1) 9.) bekövetkezése és az érintett szerv NKI általi értesítése között eltelő idő.

IT biztonságtudatosság erősítése

Projekt keretében elkészült tanulmányok

A projekt egyik kiemelt célkitűzése volt az IT biztonságtudatosság növelése és a tématerülethez kapcsolódó érzékenyítés. A fenti cél elérése érdekében a projekt keretében elkészítésre került 5 db informatikai biztonságtudatosságot elősegítő tanulmány.

- Az információbiztonság lélektana

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/az-informaciobiztonsag-lelektana/

Az információ egyre fontosabb szerepet tölt be mindennapjainkban, a társadalom egyik alappillérévé vált. Jelen van a kommunikációban, a döntéshozatalokban, valamint a különféle folyamatok, eljárások lebonyolításában is. Az információ értékének növekedésével együtt jár a különböző információk megszerzésére irányuló támadások megjelenése is, függetlenül attól, hogy az adott információ bizalmasnak tekinthető-e vagy sem.

A számítástechnikai és elektronikai eszközök tárháza szinte végtelen, és az idő előrehaladtával folyamatosan jelennek meg új és új eszközök, amelyek azonban számos veszélyt rejthetnek magukban. Az új eszközök megjelenése új támadási alternatívát, felületet is jelenthet, éppen ezért kiemelt jelentőségű, hogy megvédjük a ránk bízott információkat a jogtalan hozzáféréstől, az információk esetleges kiszivárgásától, módosításától vagy akár megsemmisítésétől. Ahhoz, hogy a védelem sikeres lehessen, nem elég csupán a támadási és védekezési módszereket ismerni, minden esetben ki kell térni a támadást végrehajtó személyek, a felhasználók, valamint a vezetők szerepére is, hiszen a védelem sikeres kialakításával sok esetben megelőzhetők a bizalmas információk megszerzésére irányuló támadások.

A tanulmány célja az emberi tényező információbiztonságban betöltött szerepének bemutatása, különösen az információ kezelésével, védelmével és megszerzésével kapcsolatba hozható személyek, mint például a felhasználók, vezetők vagy akár a támadók információbiztonsági vonatkozásának ismertetése.

- Visszaélések a kibertérben

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/visszaelesek-a-kiberterben/

Az emberiség történelme során az egyének szubjektív valóságérzékelése mindig is teremtett alternatív értelmezéseket a tényeknek és összefüggéseknek, századunkra a technológiai fejlődés hatására nemcsak alternatív értelmezéseit találjuk meg a valóságnak, hanem maga a valóság alternatív síkokon játszódik. A valós tér, a kibertér, a kiterjesztett valóság tere és a virtuális valóság tere jelenünkben, de leginkább a közeljövőben úgy kuszálódik össze, olyan hatás-kölcsönhatás mechanizmusokkal működik, amelyet egy átlagos ember nem tud ésszel felfogni, és pláne nem képes teljes mértékben kiigazodni ebben a világban.

Tanulmányunk címe: visszaélések a kibertérben, de ez a cím félrevezető, hiszen a kibertér visszaélései a valós, térbeli életünkre vannak a legnagyobb hatással, a valós, megfogható életünkben tett döntéseink pedig a kibertérbeli életünkre hatnak. Nem lehet már szétválasztani őket. A fejlődés kerekeit pedig nem vagyunk képesek visszafordítani, így meg kell találnunk azt az utat, amely ebben segítségünkre lehet. A jelen tanulmány pedig ebben kíván segíteni. A mű elkészítése során ismert híresebb és/vagy tanulságosabb gyakorlati példákat mutatunk be olyan visszaélésekre, amelyekből levonhatjuk a megfelelő tanulságokat, illetve megnézzük a tudomány és a kiberbiztonsági szakértők jelen tudásának egy csekély metszetét, hogy meg tudjuk előzni, fel tudjuk tárni vagy el tudjuk hárítani a fenyegetések nagy részét. Lebegjen előttünk azonban a közhely: „nincs tökéletes védelem", de ettől még törekedni lehet rá.

- Mobil eszközök hivatali használata

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/mobil-eszkozok-hivatali-hasznalata/

A tanulmány célja annak bemutatása, hogyan lehet hivatali környezetben a mobil eszközöket biztonságos módon alkalmazni. Példákon keresztül bemutatjuk a mobil eszközök magán és hivatali használatának veszélyeit, továbbá, hogy milyen biztonsági intézkedésekkel lehet a hivatali használat kockázatait csökkenteni. A hivatali mobil eszköz használatának eseteit külön fejezetben fejtjük ki részletesen. A tanulmány kitér a hivatali mobil eszközök biztosításának módjaira is, valamint külön fejezet szól a hivatali mobil eszközök használatának bevezetéséhez kapcsolódó stratégiákról is. Nemcsak a gyakorlati megvalósítás fontos a mobil eszközök hivatali használata során, hanem a jogi háttér vizsgálata, elemzése is, mely önálló fejezetet kapott a hatályos jogi szabályozás információbiztonsági, adatvédelmi és egyéb releváns területein keresztül. A tanulmány végén, az összegzésben összehasonlítjuk az egyes használati módok előnyeit és hátrányait, valamint a bevezetési stratégia fontosabb lépései is teret kapnak.

A tanulmány – adott keretek között – törekszik a mobil eszközök hivatali bevezetésének legszélesebb és legmélyebb aspektusait bemutatni arra is figyelemmel, hogy a téma gyorsan változik, folyamatosan bővülnek a rendelkezésre álló információk, és látnak napvilágot az alkalmazást befolyásoló biztonsági események és az arra adott válaszok. Figyelembe kell azt is venni, hogy az elemzés eredményeit egy konkrét szervezetnél történő bevezetéskor a szervezet sajátosságaira tekintettel kell felhasználni.

- Informatikai behatolások és felismerésük

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/informatikai-behatolasok-es-felismeresuk/

A tanulmány kifejezetten azt a célt hivatott elérni, hogy átfogó képet nyújtson a különböző kiberbiztonsági kihívásokról és technikákról, hiszen anélkül, hogy tudomásunk lenne a támadó oldalról, nem lehetséges védekezni. Nem célja egy-egy technika mélyebb szintű ismertetése, annak legapróbb részleteinek bemutatása. Ismertetésre kerül egy általános támadás menete a kibertérben a célpont

kiválasztásától kezdve a különböző passzív és aktív támadásokon keresztül a nyomok eltüntetéséig. Bemutatásra kerülnek a különböző malware típusok, illetve néhány közismert támadásról is szó esik. Ezeket követően különböző eszközök, technikák, információbiztonsági kontrollok használatának segítségével a védelem kialakításának idealizált kiépítésének bemutatása következik.

Fontos hangsúlyozni, hogy – mint ahogy a támadások is nagyon szerteágazó palettán mozognak – nem létezik egy olyan út, melyet követve egy szervezet teljes biztonságban lenne. Egyfelől nem létezik 100%-os védelem, másfelől minden szervezet más infrastruktúrát használ, más területen tevékenykedik, így a különböző fenyegetések mértéke eltér. Fontos látni, hogy az adott szervezet érettségi szintjének, illetve az üzleti oldal igényeinek figyelembevételével alakíthatók ki észszerűen a biztonsági védvonalak.

- Közösségi hálózatok hivatali használata

https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/kozossegi-halozatok-hivatali-hasznalata/

A közösségi oldalak használata napjainkban komoly kihívás elé állítja a szervezeteket. Bár számos biztonsági kockázatot jelentenek, megfelelő biztonságtudatos használattal a kockázatok minimalizálhatók. A közösségi oldalak számos olyan lehetőséget biztosítanak az egyes szervezeteknek, amelyek segítségével nagyban növelhetik jogszabályban meghatározott feladataik hatékony ellátását. A szervezet és az ott kezeltek adatok függvényében azonban nem csupán célszerű a közösségi oldalak használatának korlátozása, hanem elengedhetetlen. Jelenleg az egyik legjelentősebb kihívást az jelenti, hogy a közösségi média hivatali használatára vonatkozóan nem áll rendelkezésre egységes módszertan.

Az információbiztonság szempontjából elengedhetetlen, hogy a különböző szervezetek kitekintsenek saját falaikon túl, és számításba vegyék a munkavállalóik által napi rendszerességgel használt közösségi szolgáltatásokat. Az elmúlt évek azt bizonyítják, hogy a támadók szinte minden esetben felhasználják a közösségi médiából származó információkat egy-egy támadás végrehajtásához. A megváltozott helyzethez történő alkalmazkodás megköveteli, hogy az információbiztonsági tudatosság kialakítására és ezzel együtt a közösségi hálózatok használatát érintő esetleges korlátozásokra konkrét szabályzatok szülessenek a közeljövőben. A szabályozás és a korlátozás mellett a közösségi média használatának számos előnye van egy hivatal szempontjából. Ennek érdekében ki kell dolgozni a közösségi média használatát érintő stratégiákat, melyek kiemelt szerepet kaphatnak a szervezet külső kommunikációjában és az ellenséges propaganda és dezinformációs hadjáratok elhárításában.

Projekt keretében elkészült e-learning anyagok

A projekt kertében elkészített közérthető tanulmányok képezték az e-learning oktatócsomag alapját. A kifejlesztett elektronikus tananyagok gyakorlat-orientáltan vezetik végig a felhasználókat a legfontosabb biztonsági kérdéseken.

A kompetenciafejlesztésen túl az NBSZ célja az érzékenyítés, a felhasználói szemlélet formálása annak érdekében, hogy a felhasználók a biztonsági kérdéskörre ne a kényelmet csökkentő akadályként, hanem javukat szolgáló lehetőségként tekintsenek.

A tananyagok online elérhetősége: https://elearning.nki.gov.hu/

Az anyagok az NBSZ (https://nbsz.gov.hu/gazdalkodas/palyazatok) és az NBSZ NKI (https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/) oldalán szabadon elérhetőek az érdeklődők részére, az e-learning kurzusok (https://elearning.nki.gov.hu/) bárki által, térbeni és időbeni korlát, illetve regisztráció nélkül elvégezhetőek

A projekt indikátorai, eredmény mutatói

Operatív Program indikátorok

Mutató neve	Kiindulási érték	Célérték	Tényérték
	2016.02.16.	2022.03.31.	2021.10.25.
A kompetencia fejlesztésben résztvevő közszolgálati szakemberek száma	0 fő	100 fő	129 fő
A képzésben részt vevő integritás tanácsadók száma	0 fő	25 fő	47 fő
A képzést sikeresen elvégző közszolgálati szakemberek aránya	0 %	90 %	95 %

„A kompetenciafejlesztésben résztvevő közszolgálati szakemberek száma” indikátor azon közszolgálati szakemberek számát jelzi, akik az EWS rendszer felhasználói, üzemeltetői és a projekt keretében lebonyolított online EWS képzésben részt vettek.

„A képzésben részt vevő integritási tanácsadók száma” mutató az EWS rendszerbe bevont szervezetek azon integritási tanácsadóinak számát jelzi, akik az online EWS képzésben részt vettek.

A kompetenciafejlesztést követően EWS szenzorral védett intézmények üzemeltetői, IT szakemberei, integritási tanácsadói vizsgát tettek a képzés során elsajátított ismereteikről.
„A képzést sikeresen elvégző közszolgálati szakemberek aránya” indikátor mutatja az EWS képzésen sikeresen résztvevők és a kompetenciafejlesztésben összesen résztvevők arányát.

Adatszolgáltatás alá eső mutatók alakulása

EWS rendszerrel védett rendszerek száma

Mutató neve	Bázisérték	Célérték	Tényérték
	2016.02.16.	2022.03.31.	2021.12.10.
EWS rendszerrel védett rendszerek száma	0	49 db	60 db

Az NBSZ projektje keretében kifejlesztésre került EWS rendszerbe az Ibtv. 1. § (1) 14b. pontjában meghatározott elektronikus információs rendszerek kerülnek bevonásra, amelyek definíciója az alábbi -

a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy

c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.

- továbbá és a fentiekre tekintettel, amely az EWS rendszerbe önálló virtuális szenzorként rögzítésre kerül, önálló rendszerentitásként, a többi entitástól függetlenül működik és ezektől függetlenül (kvázi saját jogon és útvonalon) érhető el a nyílt internet irányából.

Az EWS rendszerbe bevont elektronikus információs rendszerek egy-egy önálló logikai szenzorral kerülnek ellenőrzésre. Az NBSZ projektje keretében 55 logikai szenzor került kialakításra, amelyek skálázható módon (a védett rendszerhez igazodó kapacitással), a védeni kívánt rendszer specifikumaihoz igazodóan (a rendszer sajátosságainak, technikai adottságainak figyelembe vételével) kerültek kialakításra és letelepítésre, úgy hogy magas számítási kapacitás és rendelkezésre állás mellett közel valós időben képesek a hálózati forgalom ellenőrzésére, ezáltal a biztonsági események, és vizsgálatot követően incidensek azonosítására.

EWS rendszerrel védett projektek száma

Mutató neve	Bázisérték	Célérték	Tényérték
	2016.02.16.	2022.03.31.	2021.12.10.
EWS rendszerrel védett projektek száma	0	20 db	22 db

Az EWS rendszerbe az NBSZ NKI által csatlakozásra kezdeményezett elektronikus rendszerek kerültek bevonásra. A védendő rendszerek kiválasztásánál prioritást élveztek a KÖFOP keretében támogatást nyert projektek. Fentiekkel összhangban tárgybani mutató esetében projektnek a KÖFOP azonosítóval rendelkező pályázat tekintendő.

Jó Állam Projekt Mutatók

Mutató neve	Bázisérték	Célérték	Tényérték
	2016.02.16.	2022.03.31.	2021.12.10.
Az EWS rendszerbe bevont KÖFOP projektek aránya	NR	100 %	100 %

A mutató az EWS rendszerbe történő csatlakozásra kezdeményezett KÖFOP projektek és a ténylegesen az EWS-be bevont KÖFOP projektek arányát ismerteti. A projekt mutató tehát a ténylegesen megvalósult EWS-be bevont KÖFOP-os fejlesztések összes EWS csatlakozásra kezdeményezett KÖFOP-os projektekhez viszonyított arányát mutatja be.

A projekt keretében létrejövő EWS rendszer és a különböző informatikai rendszerek csatlakoztatása által csökken azoknak a kiberszempontú támadhatósága (adatlopások, honlaptámadások) és a korrupciós célú belső vagy külső támadások, fenyegetettségek aránya (kémprogramok, adatlopások, rendszerzavarok kialakítása).

Mutató neve	Bázisérték	Célérték	Tényérték
	2017.01.16.	2022.03.31.	2021.12.10.
Értesítési idő csökkenése, a közigazgatási szervezetek elektronikus rendszereit érintő hálózati forgalomelemzéssel	104 óra	24 óra	0,75 óra

Értesítési idő csökkenése, azaz a közigazgatási szervezetek elektronikus rendszereit érintő hálózati forgalomelemzéssel azonosítható biztonsági esemény (2013. évi L. tv. 1. § (1) 9.) bekövetkezése és az érintett szerv NBSZ NKI általi értesítése között eltelő idő csökkenése.
Az EWS segítségével a kapcsolódott intézmények hamarabb és nagyobb mértékben szerezhetnek tudomást a támadásról, illetve ezáltal hamarabb kezdhetik meg a rendszert érintő támadások (pl. hálózati betörési kísérlet, adatlopás, weboldal rongálás), visszaélések, korrupciós cselekmények (pl. adatszivárogtatás, zsarolási kísérlet) és kockázatok (pl. sérülékeny vagy illetéktelen eszközök és szolgáltatások, lappangó kártevők) kezelését.

Az értesítési idő csökkenése elősegíti, hogy a közigazgatás EWS-be bevont szervezetei, rendszerei biztonságosabb és stabilabb környezetben működjenek (elsősorban külső - kiber - támadásoktól). Ennek eredményeképpen az újonnan kialakított EWS rendszer számos további rendszer biztonságosabb működéséhez járul hozzá.

Mutató neve	Bázisérték	Célérték	Tényérték
	2016.02.16.	2022.03.31.	2021.11.30.
Tudásformáló, IT biztonságtudatosságot erősítő anyagok használatának száma	NR	1 500 db	97 758 db

A tudatosítás hatásfokának egyik kiemelten fontos mérőszáma, hogy a projekt keretében elkészített tanulmányokat és ahhoz kapcsolódó ismertető anyagokat (kivonatok, e-learningek stb.) mennyien látják, mennyien használják fel. A tudásformáló tanulmányok és a kapcsolódó további ismertető anyagok elektronikusan megosztásra kerültek a projekt keretében (a tanulmányok pdf formátumban letölthetőek és e-learning formában is feldolgozhatóak). Ezért mérésre került, hogy a létrehozott tudásformáló anyagokat mennyien dolgozták, használták fel a projekt ideje alatt. Az NBSZ NKI oldalán mindenki által szabadon elérhető tanulmányok esetében mérésre került az anyagok letöltésének száma, mindenki által szabadon elérhető e-learning tananyagok esetében mérésre került az anyagok elindításának száma, fentiek mellett a BM RVTV portálján, a BM hivatásos, RIASZ és munkavállalói állománya részére továbbképzési programként közzétett e-learning anyagok esetében mérésre került a képzést elvégzők száma.

A szemléletformálásra irányuló tevékenység révén elérhető, hogy a közszférában dolgozók meghatározott csoportjai megfelelő információkhoz jussanak az integritás megteremtéséhez szükséges IT biztonsági ismeretekről. A tudásmegosztás és érzékenyítés által nőhet azok aránya, akik viszonyulása kedvező lehet az elektronikus ügyintézéshez.

A projekt keretében megvalósult disszemináció, kommunikáció

Disszeminációs tevékenységek

Tájékoztató rendezvény

2017.06.29-én tájékoztató rendezvény került lebonyolításra annak érdekében, hogy a KÖFOP kedvezményezettek ismereteket szerezzenek a kifejlesztés alatt álló EWS rendszerről, megismerhessék a rendszer képességeit, előnyeit, a csatlakozás előzetes felételeit.

Szakmai rendezvények

2021. első félévében három alkalommal szakmai workshop került megrendezésre, amelynek keretében az EWS rendszerrel érintett felhasználók technikai ismereteket szerezhettek a rendszer működéséről, az EWS jogszabályi hátteréről, valamint a rendszerhez való csatlakozás gyakorlati lépésieről.

Projektzáró rendezvény

A projekt eredményeinek ismertetése céljából 2021 november 24-én projektzáró online esemény került megrendezésre az EWS-hez csatlakozott intézmények, rendszerek képviselői részére.

Disszeminációhoz kapcsolódó honlap fejlesztés

Az NBSZ NKI oldalán (https://nki.gov.hu/ews/) EWS aloldal került létrehozásra, amelyen az érdeklődök ismereteket szerezhetnek a KÖFOP projekt alapadatairól, az EWS szolgáltatásról, valamint egy helyen elérhetik a projekt keretében elkészített IT biztonságtudatosság erősítését célzó tanulmányokat, e-learning anyagokat, tájékoztató kiadványokat, előadásokat.

Kiadványok

2017 első félévében tájékoztató kiadvány került elkészítésre az EWS rendszerhez potenciálisan csatlakozó védendő intézmények részére.

A fejlesztési tevékenységek lezárultát követően a projekt eredményeinek bemutatása céljából rövid ismertető, tájékoztató kiadvány került elkészítésre.

A digitális kiadványok az NBSZ-NKI oldalán (https://nki.gov.hu/ews/) elérhetők az érdeklődők részére.

Kommunikációs tevékenységek

Projekt előkészítő szakasz

Tekintettel arra, hogy a projekt kiemelt célja közvetlenül nem érinti a lakosságot, illetve a fejlesztés közvetlen célcsoportja a KÖFOP keretében kiírásra került pályázati felhívásokból tájékoztatást kapott a „Nyomtatott tájékoztatók elkészítése és lakossági terjesztése" feladat kapcsán az NBSZ egyedi felmentési kérelemmel fordult a Támogató felé.

Kommunikációs terv

A projekt előkészítési szakaszában kommunikációs terv került elkészítésre, amelyben részletesen bemutatásra került az NBSZ által a projekt keretében vállalt kommunikációs elemek tervezett megvalósítása, ütemezése a hozzárendelt forrásokkal egyetemben.

Honlap:

Az NBSZ honlapján (http://www.nbsz.gov.hu) a pályázathoz közvetlenül kapcsolódó információkat a projekt pénzügyi zárásáig közzéteszi, frissíti.

Megvalósítási szakasz

Tekintettel arra, hogy a projekt kiemelt célja közvetlenül nem érinti a lakosságot, illetve a fejlesztés közvetlen célcsoportja a KÖFOP keretében kiírásra került pályázati felhívásokból tájékoztatást kapott, valamint figyelemmel az NBSZ feladat- és hatásköréből adódó speciális jellegére a „Sajtóközlemény kiküldése a projekt indításáról", „Sajtónyilvános események szervezése", „Média-megjelenés vásárlása a projekthez kapcsolódóan" feladatok kapcsán az NBSZ egyedi felmentési kérelemmel fordult a Támogató felé.

Tájékoztató és emlékeztető táblák:

A projekt végrehajtása során az NBSZ a projekt megvalósításának helyszínein tájékoztató táblákat helyezett ki a Széchenyi 2020 Kedvezményezettek tájékoztatási kötelezettségei útmutatóban rögzítettekkel összhangban. Figyelemmel arra, hogy a fejlesztés több megvalósítási helyszínt is érintett a projekt keretében 1 db „B" és 3 db „C" tábla került kihelyezésre az NBSZ Központi és Tároló Objektumában, valamint a NISZ telephelyein.

Fotódokumentáció összeállítása

Az NBSZ biztonsági szabályainak betartása mellett fotódokumentáció került elkészítésre a képzésekről, szakmai rendezvényekről, valamint a pályázat keretében beérkezett eszközökről.

Projekt megvalósítást követő szakasz

Eredménykommunikációs információs kiadvány

A projekt sikeres megvalósításának, eredményeinek bemutatása érdekében információs kiadvány került elkészítésre.

TÉRKÉPTÉR feltöltése

A projekt végrehajtását követően a projekt megvalósítása során készített, biztonsági szempontból megfelelőnek ítélt fotók, illetve a projekt alapadatai a TÉRKÉPTÉR rendszerre feltöltésre kerültek.

Emlékeztető tábla elhelyezése

Az NBSZ központi objektumának bejáratánál 1 db „D” típusú emlékeztető tábla került kihelyezésre.

Tekintettel arra, hogy a projekt kiemelt célja közvetlenül nem érinti a lakosságot, illetve a fejlesztés közvetlen célcsoportja a KÖFOP keretében kiírásra került pályázati felhívásokból tájékoztatást kapott, valamint figyelemmel az NBSZ feladat- és hatásköréből adódó speciális jellegére az NBSZ az alábbi kommunikációs elemek tekintetében egyedi felmentési kérelemmel fordult a Támogató felé:

- nyomtatott tájékoztatók elkészítése és lakossági terjesztése,
- sajtóközlemény kiküldése a projekt indításáról,
- sajtónyilvános események szervezése,
- média-megjelenés vásárlása a projekthez kapcsolódóan.