MINISZTERELNÖKI HIVATAL

INFORMATIKAI BIZTONSÁGI FELÜGYELŐ

Részletes jelentés
a Központi Elektronikus Szolgáltató Rendszer
egyes szolgáltatásainak üzemzavarairól

2009. január 19. és február 7. között három olyan üzemzavar következett be a Központi Elektronikus Szolgáltató Rendszer szolgáltatásaiban, amelyek nagy nyilvánosságot kaptak. Az eseményekkel kapcsolatban parlamenti kérdés került benyújtásra és interpelláció hangzott el, illetve az eseményekkel kapcsolatban tájékoztatást kért az Országgyűlés Gazdasági és Informatikai Bizottságának Informatikai Albizottsága.

Az események az érintett szervezetek, valamint az informatikai biztonsági felügyelő által kivizsgálásra kerültek. Mindhárom esetben megállapítást nyertek az eseményeket kiváltó okok, és azok felelősei, és a további, hasonló eseményeket előidéző okok megelőzése érdekében az érintett szervezetek intézkedési terveket készítettek.

Az ellenőrzés során megállapítást nyert, hogy **mindhárom esemény ugyanazon okra vezethető vissza**: a nem kellő gondossággal letesztelt programmódosítások éles üzembe állítására, **a változáskezeléssel kapcsolatos – informatikai biztonság körébe tartozó – szabályok és eljárásrendek személyi mulasztás miatt bekövetkezett figyelmen kívül hagyására**.

1. esemény: OEP – 2009. január 19.

Január 19-én az Országos Egészségbiztosítási Pénztár rendszere a biztosítotti jogviszonyt az igénybevevők jelentős körénél hibásan rendezetlennek jelezte. A hiba oka egy olyan – január 17-én, szombaton telepített – programmódosítás volt, melynek keretében több javítást végeztek, de nem minden módosítás hibátlan működése lett letesztelve. A programmódosítás önmagában nem volt hibás, csak nem terjedt ki minden szempontra, és a nyugdíjasok esetében feleslegesen hajtotta végre a jogviszony-ellenőrzést, ezzel jelentősen megnövelve a rendszer számításigényét, melynek következtében a feldolgozás hétfő reggelre „nem érte utol magát”.

> A programhiba lényege az volt, hogy téves jogviszony-bejelentés észlelésénél a szoftver nem csak az adott biztosított jogviszonyát „bontotta le” és „építette fel” újra, hanem az adott foglalkoztató által bejelentett összes személy jogviszonyát is. Mivel a feldolgozásra váró addigi APEH-jelentésekben nyugdíjas biztosítottak is szerepeltek, az újrakalkulálás elindult valamennyi, a NYUFIG által korábban bejelentett tételen. A rendszer nem volt felkészülve arra, hogy ilyen nagyszámú „foglalkoztatott” adatait futtassa, ami azt eredményezte, hogy január 19-én hétfő reggelre 8 millió találatból csupán 3,5 milliót tudott lefuttatni, és a jogviszonyt helyreállítani. A többi foglalkoztatott esetében „piros jelzést” adott ki, azaz a jogviszony rendezetlenségét jelezte.

A **szoftver hibája nem akadályozta**, és nem akadályozhatta **a lakosság ellátását**, hiszen bármilyen színű lámpát jelez a jogviszony ellenőrzés, a hatályos jogszabályok alapján a szolgáltatóknak az egészségügyi ellátást és a támogatott gyógyszereket és gyógyászati segédeszközöket megkülönböztetés nélkül kell biztosítaniuk.

Az **alapadatok nem sérültek meg** – mint ahogyan azt az adatvédelmi biztos helyszínen tartott vizsgálata is megállapította – csak az úgynevezett képzett adatok nem mutatták a valós helyzetet. A meghibásodás következtében a rendszer mintegy 950 ezer személyt érintő jogviszony hiányt jelzett, amelyek kb. 4000 kivételével nyugdíjas jogviszonyok voltak.

A hibásan működő programmodult már január 19-én délben lecserélték, azonban az adatok helyreállítása, és azok helyességének ellenőrzése hosszabb időt vett igénybe, a rendszer hibátlan működéséről véglegesen január 22-én tájékoztatták a lakosságot. A tesztelés hiányosságai miatti felelősséget a fejlesztő cég elismerte, a belső vizsgálat megállapította a belső felelősök körét is.

Az események idősorrendi leírása[1]

2008. december 19.
Az OEP üzemeltetésében 2002. év óta működő biztosítotti jogviszony-ellenőrzésre szolgáló programrendszer (BSZJ-rendszer) múlt év szeptemberétől kezdődő továbbfejlesztése első ütemének lezárásaként 2008. december 19-én – a tervezett ütemben és minőségben – sikerrel zárult a programrendszer új verziójának terítése. Az alkalmazás üzemszerű működése megkezdődött.

2009. január 9.
Az első tapasztalatok alapján 2009. január 9-én, a Projekt Fejlesztő által delegált vezetője levélben jelezte, hogy a módosítás következtében a rendszer működésében ún. performancia gondok jelentkeztek. Ezek csökkentésére a rendszer finomhangolása vált szükségessé, amit a Fejlesztő két lépcsőben (január 9-én és január 16-án) végzett el.

2009. január 12.
Az OEP munkatársa bejelentett egy hibát, ami egy adatbázisban tárolt eljárás diszfunkcionalitására utalt. A kivizsgálás során kiderült, hogy a „BSZJ_JOGVISZONY" programcsomagban van a hiba, az újrakalkulációs részben. A javítás során átvizsgált kódrészleteket elemezve, programozási pontatlanságra is fény derült. (Ennek a hibának Fejlesztő általi átírása folyamán keletkezett aztán az eseménysorozatot elindító programhiba.)

2009. január 14.
Jogszabály-módosítás miatt az Adó- és Pénzügyi Ellenőrzési Hivatal (APEH) ez év január 1-jétől megváltoztatta az OEP felé teljesítendő jelentéseinek rekordszerkezetét. A módosult struktúrájú APEH-jelentések fogadásához természetesen a fogadóoldali BSZJ-t is változtatni kellett, amit a programrendszer szupportálását alvállalkozóként végző Fejlesztő elvégzett. A Projekt január 14-ei ülésén ezért elsősorban az APEH struktúra-módosítása miatti programváltoztatás bevezethetőségéről (engedélyeztetés, terítés stb.) esett szó. Említésre került tovább, hogy az új programverzió terítésével párhuzamosan az újrakalkulációs tárolt

[1] Az Országos Egészségbiztosítási Pénztár vizsgálati jelentése alapján

eljárásban észlelt hiba átírására telepítendő fájl is elkészült, amelyet a másnap átadandó, az új programverziót tartalmazó adathordozón (CD) rendelkezésünkre bocsát.
Meg kell jegyezni, hogy a Projekt üléséről készített Emlékeztető tanúsága szerint a Projekt minőségbiztosítását végző Projektiroda aggodalmát fejezte ki, hogy az új programverzió terítését megelőzően – a Fejlesztő saját fejlesztői tesztállományán való lefuttatás mellett – az OEP-en rendelkezésre álló rendszeren nem történik külön is teszt. A Felek végül megegyeztek, hogy ha hiba is történik, az adatok nem veszhetnek el, legfeljebb (a legrosszabb esetben) apróbb javításokra lehet szükség, amelyek nem zavarják a rendszer működését. Így viszont tartható az APEH-jelentések struktúra-módosítása miatti programverzió terítésére korábban célul tűzött határidő (január 20.). Az Emlékeztető alapján nem világos, ám a résztvevők elmondása szerint egyértelmű volt, hogy a Projektiroda aggodalma csak a programverzió, s nem az újrakalkulációs tárolt eljárás átírásának terítéséről szólt.

2009. január 15.
A Fejlesztő az Országos Egészségbiztosítási Pénztár szervezeti egységei és igazgatási szervei által használatba vételre tervezett alkalmazások fejlesztési, tesztelési, bevezetési eljárási rendjéről szóló 12/2005 (Eb.K.5) számú Főigazgatói Utasítás (Utasítás) előírásai szerinti formában, kellékekkel átadta a programverziót és a tárolt eljárás javítására szolgáló, telepítendő fájlokat tartalmazó adathordozót.

Az átvételt követően a Nyilvántartási és Ügyvitelszervezési Főosztály (Szakfőosztály) munkatársa ez alapján elkészítette a funkciótesztről szóló dokumentumot, melyet munkatársa ellenőrzött, és a Szakfőosztály főosztályvezető-helyettese (aki azon a héten a távollévő főosztályvezetőt helyettesítette) jóváhagyta. **A funkcióteszt célkitűzéseként csak „Az új XML formátumú 2009-es APEH jelentések fogadása és feldolgozása" szerepelt, a tárolt eljárás javítása nem.**

2009. január 16.
A terítési engedély birtokában a Fejlesztő 2009. január 16-án készre jelentette, és telepítési csomagban (mennyiségi átadás) átadta az OEP-nek a programcsomagot. **Az új verziót január 16-án, pénteken 19:30-kor töltötték be az éles BSZJ-rendszerbe. A program rendben elkezdett futni, hibára nem derült fény**, ezért mind a munkatársak, mind a Fejlesztő munkatársai hazamentek hétvégére.

2009. január 17.
A 2009. január 16-án végrehajtott terítésben szereplő programhiba következtében január 17-én, szombaton elindult a NYUFIG általi bejelentések (mintegy 8,2 millió tétel) újra-feldolgozása.

2009. január 19.
Munkaidő kezdetekor a Szakfőosztály jelzést kapott arról, hogy a Regionális Egészségbiztosítási Pénztárak (REP-ek) munkatársai hibát észlelnek a program indításakor, továbbá az egészségügyi szolgáltatóknál és a gyógyszertárakban olyan állampolgároknak is rendezetlen jogviszonyt jelez a jogviszony ellenőrző rendszer, akik ténylegesen érvényes jogviszonnyal rendelkeznek.

A hiba okának keresését haladéktalanul megkezdték, és megállapították, hogy a TAJ-BSZJ rendszer, az újonnan fejlesztett jogviszony újra-kalkulációját végző szoftver hibája és a hétvégén fellépő – a nagy tételszámú feldolgozásból eredő – technikai hiba miatt a

jogviszonyokat lebontotta (pirosra állította), majd a jogviszonyok újraképzésének folyamata megszakadt.

Erről a tényről azonnal értesítették a Fejlesztő szakembereit, és kérték a hiba azonnali javítását. Az OEP Számítástechnikai Üzemeltetési Főosztály (SZÜF) adatbázis adminisztrátorainak és a REP-ek szakosztályai felé is jelezték, hogy a hiba javítása folyamatban van.

Tizenegy órakor fejlesztőtől írásban is kérték a hiba okának megállapítását és a javítás határidejének megjelölését. Eközben a javítóprogram megérkezett, ennek lefordítása azonban csak leállított rendszer esetén volt lehetséges. Miután a REP-eknek **12 órakor a leállítást jelezték, néhány percre, a fordítás időtartamára a rendszert leállították. Ezt követően a hibás működés megszűnt, és az adatok javítása megkezdődött.** A hiba okáról és a javítás menetéről a SZÜF-öt értesítették.

A meghibásodás következtében a rendszer 5 144 244 tétel (számításaink szerint, mintegy 950 ezer személyt érintő) jogviszony hiányt jelzett, zömében feltehetően hibásan. **Ezek – kb. 4000 kivételével – nyugdíjas jogviszonyok voltak**. Világossá vált az a tény, hogy a súlyos hiba javítását követően a jogviszonyok helyreállítása rövid időn belül nem valósulhat meg, ezért a jogviszony-ellenőrzést végző gyógyszertárak és egészségügyi szolgáltatók értesítése a VIREP-en (gyógyszertárak) keresztül 14:03-kor, míg az OJOTÉ-n keresztül (egészségügyi szolgáltatók) 16 órakor megtörtént.

2009. január 20.
Reggelre a hibajavítást követő jogviszonyrendezés ismeretlen okok miatt elakadt, így 2009. január 20-án munkakezdéskor még a rendszer nem volt működőképes (3,1 millió feldolgozatlan tétel maradt és nagyon lassan ment a feldolgozás). Ennek ismeretében az EüM-ben tartott megbeszélésen azonnali, rendkívüli sajtótájékoztató megtartása mellett döntöttek. A 10 órára összehívott sajtótájékoztató megszervezésével egyidejűleg tájékoztató közlemény jelent meg az OEP-honlapon, illetve az egészségügyi szolgáltatók felé újabb tájékoztatást juttattak el az OJOTÉ-n és a VIREP-en keresztül.

Fejlesztő jelezte, hogy új algoritmust dolgoztak ki, és ennek eredményeképpen a jogviszonyok rendezése a nap végére – terveik szerint – befejeződik.

2009. január 21.
Reggel 7:30-kor a Fejlesztőtől azt a tájékoztatást kaptuk, hogy előző este 10 óra környékére az adatbázisban található "zöld lámpák" megfelelő (valóságot tükröző) helyzete 99%-ig visszaállt. A maradék 1% (kifejezetten egyedi esetek) bedolgozása folyamatosan történik, de az rendkívül idő- és erőforrás-igényes folyamat.

Az intézmények szondázása és a REP-ek ügyfélszolgálati jelzései továbbra is a jogviszony-ellenőrzési rendszer hibás működését valószínűsítették, ezért 14 órakor arról értesítettük a sajtón, illetve a honlapunk lakossági és szakmai oldalán keresztül az érintetteket, hogy a folyamatos munka ellenére sem sikerült ez ideig a jogviszony-ellenőrzési rendszer adatbázisában keletkezett hibát megnyugtató módon kijavítani.

Délelőtt a Projekt soron következő ülésén úgy döntöttek, hogy az eladdig fel nem dolgozott maradék nyitott tétel helyett a Fejlesztő – az OEP munkatársaival folyamatosan egyeztetve – úgynevezett „okirati nyitó tételt” generál (az ügyintézőknek van lehetőségük ilyen tételt

generálni az ügyfélszolgálatokon, ha úgy ítélik meg, hogy az adott személynek kell lennie nyitott jogviszonyának). A „zöldre állítás” 12 órára befejeződött.

Délután az Adatvédelmi Biztos Irodájának szakemberei helyszíni vizsgálatot tartottak az OEP-ben a történtek tisztázása céljából. Az egyeztetésről már másnap kézhez kaptuk az Emlékeztetőt, amelynek legfontosabb megállapítása: adatvédelmi szempontból megnyugtató, hogy az adatbázisban szereplő személyes adatok nem sérültek a hiba folytán, adatvesztés nem történt.

2009. január 22.
Reggeltől kezdődően a REP-ek vezetőitől folyamatosan kaptuk a nyugtázó válaszokat a rendszer zavartalan működéséről, ám a visszacsatolási folyamat megnyugtató lezárására csak délután 16 órára került sor.

Fentiek eredménye a közzétett sajtóközleményünk, amely szerint az OEP a jogviszony-ellenőrzési rendszerben keletkezett hibát kijavította, így a január 22-étől az ellenőrzés ismét zavartalanul működik.

A Fejlesztővel tartott megbeszélésen – tekintettel arra, hogy kizárólag a Fejlesztőnek felróható hibás teljesítés nem állapítható meg, a keletkezett hibáért az OEP is részben felelős; továbbá arra, hogy az okozott hiba, és az ebből eredő esetleges anyagi kár nem, vagy nagyon nehezen számszerűsíthető – a felek közös megegyezéssel eltekintettek a kártérítés anyagi jellegű érvényesítésétől, azonban **megállapodtak további fejlesztői embernapok Fejlesztő általi térítésmentes biztosításáról és a terítések során szükséges folyamatos fejlesztői jelenlétről**.

Felelősség megállapítása, intézkedési javaslatok

Leszögezve, hogy a biztosítási jogviszony-ellenőrzési rendszer meghibásodását közvetlenül a Fejlesztő által elkövetett programhiba okozta, a Jelentés megállapításait összegezve a bekövetkezett hiba előidézésében, annak kezelésében az alábbi közvetlen és közvetett felelősség körök, és az azokhoz kapcsolható intézkedési javaslatok fogalmazhatók meg:

Felelősségi megállapítások

- a terítendő programverzió és az újrakalkulációs tárolt eljárás javítását szolgáló fájl tesztelésének mellőzéséről szóló projektdöntés nem vette figyelembe a minőségbiztosítást végző Projektiroda ezzel kapcsolatos aggályát, az ellentétes volt az irányadó Utasítással. A bekövetkezettek ismeretében ez mindenképpen hibás döntésnek minősíthető, ebben **közvetlen felelősség terheli az OEP és a Fejlesztő által delegált mindkét projektvezetőt, és közvetett felelősség terheli a Projektben résztvevő valamennyi munkatársat**;

- a Fejlesztő által átadott adathordozón tárolt telepítendő fájlok engedélyeztetési eljárásakor a – Projekt által hozott szabálytalan döntésnek megfelelve – **elmaradt a funkcionális teszt lefuttatása**. Ennek ellenére született, a terítési engedély megadásához megkövetelt, eredményes teszt-jegyzőkönyv, de csak az APEH jelentés-struktúra módosítását kezelő programverzióra, a tárolt eljárás javítását szolgáló programra nem. A változáskezelési előírások nagyvonalú kezelése tette lehetővé a hibás programkód megfelelő tesztelés

nélkül történő éles rendszerbe való implementálását, illetve egy verzióváltás mellett egy időben több különböző programfunkciót érintő változtatást a rendszerben. Ebben **mind a jegyzőkönyv elkészítésében, mind annak ellenőrzésében, illetve jóváhagyásában résztvevőket közvetlen és közvetett felelősség terheli**;

- a hiba felismerését, meghatározását és annak elhárításának azonnali megkezdését követően a programrendszerben ezzel párhuzamosan nem történt visszaállás a pénteki, utolsó mentett állapotra. Ezt a döntést a szakfőosztály vezetőjének tájékoztatása alapozta meg, amely szerint a programrendszer teljes „felzárkózásának" valószínűsíthető idő- és erőforrásigénye jelentősen meghaladta volna a programjavítás akkor becsülhető időszükségletét. **Az üzletmenet-folytonossági terv, a katasztrófa-elhárítási terv, valamint az informatikai biztonságot érintő vészforgatókönyv nem teljes körűsége, egyéb elemeinek hiánya miatt közvetett felelősség állapítható meg**;

- **a tájékoztatási folyamat nem kielégítő volta mutatott rá az értesítési csatornák nem teljes körűségére**. Hiányzik a – többek között a biztosítási jogviszony-ellenőrzést is végző – OEP-pel szerződött egészségügyi szolgáltatók közvetlen (tehát nem a rendszergazdákon keresztüli) elérését szolgáló hiteles, online karbantartott adatbázis. Ilyen irányú kötelezettséget jogszabály vagy egyén norma nem ír elő, **ezért felelősség nem megállapítható, ám a kiépítése elemi érdekünk**;

- az érintett főosztályok közötti hosszú hónapok egyeztetéseinek eredményeképp **létrejött a programrendszer fejlesztéséhez elengedhetetlen OEP-en belüli tesztkörnyezet, ám a valóban elvárható teljes funkcionalitású, minden külső kapcsolattal is rendelkező, „éles" tesztrendszer a mai napig nem került kiépítésre**. Ennek részben oka, hogy több év infrastrukturális lemaradását kell behoznunk.

Az informatikai biztonsági felügyelő ellenőrzése

Az informatikai biztonsági felügyelő 2009. február 3-án az előzetesen jóváhagyott éves ellenőrzési terve alapján célellenőrzést hajtott végre az Országos Egészségbiztosítási Pénztárnál, amelynek keretében vizsgálta a január 19-én bekövetkezett események okait is.

Az ellenőrzés főbb megállapításai:

Az OEP informatikai biztonsággal összefüggő szabályrendszere és informatikai biztonsági helyzete rendszeresen auditálásra, ellenőrzésre kerül. Ez az elmúlt év folyamán is megvalósult, a felügyeleti szerv (EÜM) megbízásából független, külső szakértő végezte el. A magas szintű biztonság fenntartása érdekében jelenleg is folyamatban van az informatikai rendszer sérülékenység-vizsgálata.

Az ellenőrzés során megállapítást nyert, hogy a szervezet – tartalmát tekintve – az informatikai biztonsági események kezelésére vonatkozóan minden olyan szabályzattal rendelkezik, amelyeket jogszabály előír. Az önálló kötetben kiadásra kerülő informatikai katasztrófa-elhárítási terv (IKET) előkészítés alatt áll, tartalmi elemeit az „Informatikai Biztonsági Politika" az „Informatikai Biztonsági Szabályzat", valamint „Számítóközpont üzemeltetési szabályzat" jelentős részben lefedik. Az informatikai okokra visszavezethető események kezelésére a jelenleg is rendelkezésre álló dokumentumok megfelelő eljárásrendeket tartalmaznak, továbbá a más okból bekövetkező katasztrófahelyzetek esetére

(tűzkár, vízkár, betörés) a „Számítóközpont üzemeltetési szabályzat” ad iránymutatást. Az IKET, mint önálló dokumentum hiánya nem játszott szerepet a 2009. január 19-i esemény kezelésében.

A számítóközpontban bekövetkező rendkívüli helyzetekben szükségessé váló munkaidőn túli munkavégzésre egyfajta riadólánc került kialakításra. A 2009. január 19-i esemény során az eszkalálási rend megfelelően működött.

Az informatikai biztonsági felügyelő jelentésében javaslatokat fogalmazott meg a hasonló események megelőzésére, illetve kezelése érdekében, amelyeket az OEP az általa készített intézkedési tervbe beépített.

Az OEP által készített intézkedési javaslatok

1. A változáskezelés szigorúbb ellenőrzése és betartatása. A tesztkörnyezetben az éles rendszerrel megegyező adatstruktúra mellett azonos mennyiségű és minőségű tesztadatok alkalmazása. Ezzel biztosítható, hogy az új verzió hibái még a tesztüzemben felismerésre kerüljenek.
   Határidő: azonnal, illetve 2009. április 5.

2. Javasolt a felhasználók (munkavállalók) részére az informatikai rendszer használatával kapcsolatos jogokat és kötelességeket tartalmazó kivonat készítése a meglévő szabályzatokból, amely a felhasználók tudomására hozza többek között a rendszer használatához kapcsolódóan rögzítésre kerülő adatok körét.
   Határidő: 2009. június 30.

3. Az OEP a jogszabályban előírt informatikai biztonsággal összefüggő dokumentumokat, szabályzatokat a 84/2007. (IV. 25.) Korm. rendelet 4.§ (2) d) pontja, illetve 7. § (5) bekezdése szerint jóváhagyásra terjessze fel az informatikai biztonsági felügyelőnek.
   Határidő: 2009. december 31.

4. Készüljön el az Informatikai Katasztrófa-elhárítási Terv. Az OEP infrastruktúra kritikus voltára tekintettel javasolt, hogy az IKET tartalmazza a 84/2007. (IV. 25.) Korm. rendelet 2. melléklet 3.17.1 pontja szerinti I. és II. kategóriájú biztonsági esemény bekövetkezte esetén az informatikai biztonsági felügyelő tájékoztatását.
   Határidő: 2009. december 31. (a jelentéstételre vonatkozó rész azonnal)

5. Az OEP a meglévő, informatikai biztonsággal összefüggő dokumentumait a kiadásuk óta megjelent KIB 25. számú Ajánlása alapján tekintse át, és az összhang érdekében a szükséges módosításokat a dokumentumokon végezze el.
   Határidő: 2010. június 30. (tekintettel az előkészületben álló informatikai biztonságról szóló törvény-tervezet hatálybalépésének idejére)
6. Javasolt az üzemeltetésben résztvevők számára a változáskezelési eljárások, illetve a rendkívüli helyzetekben követendő eljárásrend időszakos felfrissítése konzultációk vagy továbbképzés keretében.
   Határidő: folyamatos

A fenti intézkedési javaslatok végrehajtására az OEP informatikai területéért felelős főigazgató-helyettese lett kijelölve.

2. esemény: Központi Rendszer lassulása – 2009. január 20.

Január 20-án, az APEH 7 féle adó- és járulékbevallási határnapján a felhasználók a rendszer jelentős lassulását érzékelték, amelyet az egyidejűleg bejelentkező felhasználók nagy száma okozott. A torlódások miatt a Központi Rendszer üzemeltetője 16.00-kor átállt a magyarorszag.hu portál kifejezetten ilyen esetekre előkészített „gyorsított dokumentumfeltöltési" üzemmódjára. Ennek lényege, hogy a határidőhöz kötött ügyfélkapus ügyintézések közvetlenül végezhetők, a portál többi szolgáltatásához a hozzáférés (például jogszabálykeresőhöz és egyéb tájékoztató, információs szolgáltatásokhoz) ebben az üzemmódban nem lehetséges.

Erre a megoldásra, amelyet a 300.000 regisztrált felhasználóra méretezett ügyfélkapu igénybevételének jelentős növekedése miatt kellett kialakítani, működésének ideje alatt – 2006. május 1 óta – összesen csak 4 alkalommal, legutóbb 2008. május 20-án kellett sort keríteni. A megnövekedett igénybevételt a rendszer ezzel a módszerrel minden korábbi alkalommal zökkenőmentesen ki tudta szolgálni.

2009. január 20-án ebben a gyorsított dokumentumfeltöltési üzemmódban nem működött az a „Java-ablakban" használható alkalmazás, amely lehetővé teszi a könyvelőknek, hogy az egyenkénti dokumentumfeltöltés helyett az összes általuk könyvelt cég adatait egyszerre, egy „kattintással" küldhessék el (egy könyvelő cég gyakran 50-100 cég könyvelését is végzi).

A problémát az okozta, hogy a „Java-ablak" alkalmazásának engedélyezését egy korábbi (2008. őszén végzett) tesztelés során letiltották, majd ezt követően nem állították vissza, így a bevallásokat csak egyenként lehetett beküldeni, amely jelentősen megnövelte az egy felhasználó által generált forgalmat. Az üzemeltető személyzet a hiba keresése során erre a lehetőségre nem gondolt. A helyzetet súlyosbította, hogy a felhasználók tájékoztatására szolgáló kommunikációs rendszer sem működött, így a lassulásról szóló üzenetet sem tudták a képernyőn megjeleníteni. Ennek oka ugyancsak egy korábbi tesztelést követő nem megfelelő konfiguráció visszaállítás volt. A hibás működésről, és az adóbevallási határidő 1 napos meghosszabbításáról szóló tájékoztatást a normál üzemmódra 20.30-kor történő visszaállítást követően is csak több órával később 23.14-kor jelentették meg.

A kelleténél lassúbb működés ellenére január 20-án 280.457 bevallás került beküldésre, amely az ügyfélkapu történetének ötödik legnagyobb dokumentumfeltöltése volt. A gyorsított dokumentumfeltöltés működése esetén a január 20-i forgalom is zökkenőmentesen lezajlott volna, amit az is bizonyít, hogy ezzel a módszerrel a korábbi alkalmakkor 360 ezer körüli, az eseményt követően 2009. február 11-én 485 ezer, 12-én pedig 783 ezer dokumentum feltöltésére került sor.

A lassulás nem járt sem adatvesztéssel, sem illetéktelen adatokhoz történő hozzáféréssel. A működés lassulása a tesztelési és az üzemeltetési szabályzat több pontjának megsértése miatt következett be, amelyek kivizsgálására, a feltárt hiányosságok kiküszöbölésére és a szükséges intézkedések meghozatalára az informatikáért felelős kormánybiztos január 30-án kelt levelében felhívta a Kopint-Datorg Zrt. vezérigazgatójának figyelmét.

A problémák fő okai és javaslatok azok megszüntetésére

A rendelkezésre álló információk (Kopint Datorg jelentése, a forgalomról szóló statisztikai adatok, valamint a Median WebAudit statisztikái) alapján 2009. 01. 20-án a Központi rendszer működése során jelentkezett problémák alapvetően a következő okokra vezethetők vissza (az okokat megalapozó tények részletes bemutatása „Tények és megállapítások" részben található).

Összegzett megállapítás:

Az óránként beérkezett dokumentumok számának tényadatait, valamint a független Median WebAudit technikai statisztikáit figyelembe véve összességében megállapítható, hogy a rendszer a nap folyamán, terhelhetőségének csúcsa közelében, a megszokottnál nehezebben elérhetően, de folyamatosan működött. Teljes leállására 22.58-kor, 14 perc időtartamban került sor, arra az időre, amíg felhelyezésre került a bevallási határidő 1 napos meghosszabbításáról szóló tájékoztató.

A folyamatos, csúcsközeli működést bizonyítja, hogy a nap folyamán a rendszer az eddigi – 997 napos – működésének 6. legmagasabb dokumentumfeltöltési eredményét produkálta. Az Ügyfélkapura 578.036 felhasználó jelentkezett be, amely a 3. legnagyobb felhasználó szám volt. Ezek az adatok egyben azt is jelzik, hogy a rendszer a 2009. 01. 20-i terhelésnél magasabb forgalmat is képes volt már kiszolgálni.

Ugyanakkor 16.00 és 20.30 között egy, a dokumentumok csoportos beküldését támogató segédalkalmazás elérhetetlensége miatt csak az egyenkénti dokumentumfeltöltés működött, amely jelentős mértékben megnövelte a rendszer igénybevételét, és ebben az időszakban csökkentette a feltölthető dokumentumok mennyiségét.

A felhasználói elégedetlenséget – és az ennek köszönhető sajtónyilvánosságot – a rendszer csökkentett működőképességéről, valamint a bevallási határidő meghosszabbításáról szóló tájékoztatás késedelmes felhelyezése generálta.

Az elkövetkező bevallási csúcsidőszakokban a hasonló problémák elkerülése érdekében a bevallási csúcsot jelentő napokra történő alaposabb felkészülés, a rendszerkomponensek – különösen beleértve a B-terv oldal komponenseit – működőképességének tesztelése, valamint a folyamatos és gyors felhasználói tájékoztatás – üzemeltetési szabályzatban leírt – eljárásrendjének áttekintése, szükség esetén aktualizálása, és gyakorlatban történő megvalósítása szükséges.

A feljegyzésben felmerült kérdések tisztázása, a felelősségek megállapítása, valamint a hasonló események elkerülése érdekében szükséges teendők meghatározása érdekében a Kopint Datorgnál részletes, minden körülményre kiterjedő vizsgálat lefolytatását látom szükségesnek a tevékenységet felügyelő MeH Infokommunikációs és E-közigazgatási Szakállamtitkárság munkatársainak bevonásával.

Tények és megállapítások

Az események kronologikus sorrendben:

A 16.00 óráig terjedő időszak:

A Kopint-Datorg által rendelkezésünkre bocsátott jelentések, a Központi Rendszer terheléséről naponta készülő statisztikák, valamint a rendszer terheltségét figyelő független WebAudit statisztikái alapján elemezve a végrehajtott tevékenységeket, és a lehetséges okokat, az alábbiak állapíthatók meg.

A Központi Rendszert érő 2009. január 20-i terhelés az eddigi csúcsok közelében mozgott, de szinte minden paraméter tekintetében érte már ennél magasabb terhelés is a rendszert:

A nap folyamán beadott bevallások száma: 280.457, amely a 997 mért nap közül a 6. legmagasabb. Ennél több bevallást nyújtottak be 2007-ben és 2008-ban február 12-én, és február 15-én, valamint 2009. január 12-én (360.947, 358.393, 345.391, 297.201, 284.934 darabot). Ezek közül a 2009. január 12-i dokumentumfeltöltési mennyiség a B-tervre átállást nem igényelte!

Az óránként beadott bevallások számát tekintve 14-15 óra között 26.806 bevallást fogadott a rendszer, amely történetének 2. legmagasabb óránkénti teljesítménye volt, ennél több 2008.02.12-én 15-16 óra között 29182 volt. A mostanihoz megközelítően ennyi bevallást fogadott a rendszer (26.587, illetve 26.254 darab) 2008. 02.12-én 16-17, illetve 14-15 óra között.

Az ügyfélkapuba bejelentkezettek száma 2009. 01. 20-án 578.036 volt, amely a 3. legnagyobb felhasználó szám, közülük 316.694 felhasználó a Magyarorszag.hu oldalon keresztül lépett be, amely az eddigi legmagasabb volt a 997 nap közül.

Figyelemre méltó tény, hogy a mostanit megelőzően a B-tervre átállásra utoljára 2008. május 20-án került sor.

A Kopint Datorg által készített jelentés szerint 15 óra körül a terhelés olyan mértékűre nőtt, amely már a kritikus szint közelében volt, ezért 15.46-kor javasolták a „B”-tervre történő átállást. A terhelés növekedését alátámasztja a WebAudit terhelési grafikonja, amelyből kitűnik, hogy 14.35-től kezdődően a válaszidők jelentősen megnőttek, és – nem kritikus mértékben, de – több alkalommal időtúllépések jelentkeztek. A rendszer ekkor még elérhetőnek volt tekinthető. A „B”-tervre átállás 16.00-kor az előírások szerint szabályosan, és rendben megtörtént. A 16.00 óráig végrehajtott feladatok esetében kifogásolható intézkedés, tevékenység nem történt. A 13-16 óráig terjedő időszakban beérkezett adóbevallások száma óránként: 23205, 26806, 22087.

A 16.00-20.30-ig terjedő időszak:

A **„B”-terv időszaka** alatt (16.00-20.30-ig) a rendszer magas terhelés mellett, de a felhasználók számára elérhetően működött. A Kopint-Datorg jelentése szerint 16.20-kor érkezett az első jelzés arról, hogy a JAVA-s dokumentumfeltöltés (amely a könyvelő számára több cég bevallásának egy csomagban történő, egyidejű elküldését tette lehetővé) nem működik. Ebben az időszakban csak az egyszerűsített dokumentumfeltöltés, amely egyidejűleg csak 1 bevallás elküldését teszi lehetővé, volt elérhető.

A beérkezett adóbevallásról szóló számadatok – amelyek szerint 16 és 20 óra között az előző órák bevallási darabszámainak csak közel fele (10075, 12158, 13499, 14209) érkezett be – azt valószínűsítik, hogy a JAVA-dokumentumfeltöltő alkalmazását használni kívánók folyamatosan próbálkoztak az alkalmazás elérésével, ezzel is terhelve a rendszert. Amennyiben ismert lett volna előttük, hogy csak az egyszerűsített dokumentumfeltöltés működik, akkor azt vették volna igénybe, és a rendszerbe a korábbi óráknak megfelelő, vagy azt meghaladó számú bevallás érkezett volna.

A bevallások számát mutató statisztikai adatoknak a szokásostól eltérő drasztikus csökkenése – más hibajelzés hiányában is – már önmagában jelzés lehet arra, hogy a rendszer működésében valami probléma van, ezért lenne fontos annak biztosítása (amennyiben ez technikailag lehetséges), hogy az üzemeltetés számára ezek a statisztikák online módon folyamatosan a rendelkezésükre álljanak.

A 20.30-23.10-ig terjedő időszak

A „normál" üzemmódra visszaállásnak a Kopint jelentése szerint is az volt az elsődleges mozgatórugója, hogy kikerülhessen az állampolgári tájékoztatás a JAVA-s dokumentumfeltöltés több mint 1 órát meghaladó hibájáról, és ezért a bevallási határidő 1 nappal történő meghosszabbításáról.

A normál üzemmódról visszaállásról a döntés 20.05-kor született meg. **A kiírásra kerülő első tájékoztató szöveg megírása 20.48-21.38-ig (50 perc!) tartott,** a kihelyezésre az engedélyt 21.53-kor kapták meg. **21.38-kor értesítés ment a szöveg kihelyezésének igényére, amire azonnal válasz érkezett, hogy a szerkesztőségi rendszer sem kívülről, sem belülről nem elérhető.** 22.40-kor a szerkesztőségi rendszer működőképes állapotba került, és **23.10-re a tájékoztatás a határidő meghosszabbításáról felkerült a honlapra**.

Részletes megállapítások:

Az infokommunikációért felelős kormánybiztos az informatikai biztonsági felügyelő vezetésével vizsgálatot rendelt el, amely az alábbiakat tárta fel.

1. 1. **A rendellenesség fő okaként a „B-terv" oldali Java-segédalkalmazás (csoportos dokumentumfeltöltő) – konfigurációs hiba miatti – működésképtelensége jelölhető meg**. A „B-terv" rendeltetésszerű működése esetén a rendszer nagy valószínűséggel képes lett volna a felhasználói igények kielégítésére, mint ahogyan arra több más alkalommal – a 2009. január 20-ainál nagyobb terhelésnél is – sor került.

   A konfigurációs hiba a rendszerben (valamely alkalmazásban) korábban történt módosítás után elmaradt, vagy nem megfelelően végzett tesztelés következménye. A hibás konfigurálásért, valamint a teszt elmaradásáért, vagy nem megfelelő végrehajtásáért felelős személy belső vizsgálat alapján egyértelműen megállapítható.

2. **A felhasználók tájékoztatására – a rendszer csökkent működőképességéről – a „B-terv" oldalán nem nyílt lehetőség**. A tájékoztató szöveg a hiba jelentkezésétől számított 7 óra, a sikertelen hibajavítási kísérlet után 5 óra múlva került csak ki. Ez a tény jelentősen hozzájárult a felhasználói elégedetlenséghez, amely sajtócikkek megjelenéséhez, parlamenti kérdéshez és interpellációhoz vezetett.

A felhasználói tájékoztatás „B-terv” oldalon történő megjelentetését akadályozó tényezők pontos oka a Kopint-Datorg által készített jelentésből egyértelműen nem állapítható meg. Ennek feltárására, és a felelősség megállapítására a Kopint-Datorgon belül belső vizsgálat szükséges.

3. **A felhasználók tájékoztatását tovább késleltette, hogy a normál üzemmódra visszatérést követően a szerkesztőségi rendszer – ugyancsak konfigurációs hiba miatt – sem kívülről, sem belülről nem volt elérhető**.

   A konfigurációs hiba egy előzetes, a rendszer minden elemére kiterjedő teszt során feltárható és kiküszöbölhető lett volna. A hibás konfigurálásért, valamint a teszt elmaradásáért, vagy nem megfelelő végrehajtásáért felelős személy belső vizsgálat alapján egyértelműen megállapítható.

.

4. **A határidő hosszabbításról szóló tájékoztató SMS késedelmesen (másnap reggel), és nem a teljes érintetti kör részére került megküldésre.** A határidő hosszabbítás a Központi Rendszer más szolgáltatásait is érintheti, függetlenül azok aznapi forgalmától, és esetleges jogkövetkezményeitől.

   Ennek okát és körülményeit ugyancsak a Kopint Datorgnál végzett vizsgálatnak kell feltárnia.

A fentebb felsoroltakra kiterjedő belső vizsgálat lefolytatására, és a felelősség megállapítására az infokommunikációért felelős kormánybiztos utasította a Kopint-Datorg Zrt. elnök-vezérigazgatóját, és a vizsgálat eredményéről 2009. február 6-ig kért tájékoztatást. A kormánybiztos egyidejűleg javaslatokat fogalmazott meg a Kopint-Datorg vezetése számára.

Az infokommunikációért felelős kormánybiztos
2009. január 29-i intézkedési javaslatai a Kopint-Datorg Zrt.
elnök-vezérigazgatója számára:

A fentebb felsorolt hiányosságok kiküszöbölése, valamint a 2009. január 20-i rendellenességek megelőzése érdekében az alábbi intézkedések megtételét, és eljárásrend bevezetését tartom szükségesnek, amellyel a következő bevallási határnapokon mérsékelhető a rendszer hibás működéséből és a tájékoztatás hiányából fakadó kockázat.

2009. február 6-ig végrehajtandó tevékenységek

1. Az üzemeltetési szabályzat szerinti üzemzavar esetén történő eljárásrend ismeretét ellenőrizni kell. Az ott leírtak szerinti működésről a Helpdesk összes lehetséges döntéshozójának oktatást kell tartani és vizsgajegyzőkönyvet kell felvenni, amely tanúsítja az ott leírtak ismeretét.

2. El kell készíteni, illetve aktualizálni szükséges a rendelkezésre álló információk alapján lehetséges sablonokat, amelyek, mint tájékoztató üzenetek kikerülhetnek a Kormányzati Portálra.

3. Ellenőrizni kell, hogy a B tervre áttérésről/visszatérésről szóló tájékoztatásban szereplők névsora megfelelő-e (az újonnan csatlakozott intézményekkel aktualizálni kell).

Csúcsidőszakot jelentő határnapok előtti tevékenységek

1. A bevallási csúcsot jelentő napokra történő alaposabb felkészülés, a rendszerkomponensek –beleértve a B-terv oldal komponenseit, valamint a folyamatos és gyors felhasználói tájékoztatást biztosító szerkesztőségi rendszer – működőképességének tesztelése szükséges.

Ennek végrehajtására a bevallási csúcsot jelentő határnapok előtti leállási ablak (amennyiben a határnap hétfőre vagy keddre esik, akkor az azt megelőző leállási ablak) igénybe vételét javaslom. Ha ez egy korábbi határnappal ütközik, akkor a MeH részéről felügyeletet gyakorló illetékes vezetővel egyeztetés szükséges. A tesztelést egy hónapon belül több alkalommal csak akkor kell az újabb határnap előtt elvégezni, ha időközben a rendszerben vagy bármely alkalmazásban módosítás történt.

A tesztelés során – a működőképesség ellenőrzése mellett – az alábbiakra kell figyelemmel lenni:

- A normál site (www.magyarorszag.hu) esetleges lassulását/túlterhelését szimulálva a Helpdesk jelzésétől számított mennyi időn belül kerül a rendszer a B terv állapotába
- A B terv tökéletes működésének ellenőrzése.
- A terheléselosztók pontos beszabályozásának ellenőrzése (szimmetrizálás).
- A lokális hibák kezelésének gyakorlása (egyenkénti újraindítás).
- Az állapotjelzések értelmezésének gyakorlása.

A bevallási csúcsot jelentő határnapokra történő felkészülés során ellenőrizni kell, hogy a B-tervre átállásról/visszatérésről szóló tájékoztatást, valamint a határidő hosszabbítással kapcsolatos információt kapók listája aktualizált-e (az újonnan csatlakozott intézményekkel, amelyeknél már legalább 1 dokumentum elküldésre került aktualizálni kell).

2. A felhasználói tájékoztatás – üzemeltetési szabályzatban leírt – eljárásrendjének áttekintése, szükség esetén aktualizálása, és gyakorlatban történő megvalósítása szükséges.

Ennek keretében az alábbiakra kell figyelemmel lenni:

- Az esetleges hibát szimulálva a Helpdesk jelzésétől számított mennyi időn belül kerül ki a megfelelő információ a Kormányzati Portálra, ha a hiba jellege olyan, hogy ott kell hibaüzenetet megjeleníteni.
- A B terv esetleges lassulása/hibája folytán mennyi idő alatt lehet a B terv oldalára kirakni a megfelelő információt.

3. A csúcsidőszakot eredményező határnapokra történő előzetes felkészülés biztosítása érdekében a legnagyobb forgalmat lebonyolító csatlakozott intézmények (különösen

az APEH, VPOP, ONYF) kapcsolattartásra kijelölt személyeitől legalább negyedévente e-mailen be kell kérni, hogy az adott hónap(ok)ban mely napokon várható csúcsterhelés, ezeken a napokon nagyságrendileg milyen terheléssel kell számolni mind le, mind feltöltési irányban. Az APEH bevallási határnapjai esetében a megadott értékektől függetlenül – amennyiben azok alacsonyabbak az előző év azonos időszakának tényadataitól – a kockázat minimalizálása érdekében az előző év adatait is figyelembe kell venni.

4. A csúcsidőszakot eredményező határnapokra készüljön ügyeleti/készenléti rend. Az ügyeletben (készenlétben) szereplő munkatársakat úgy kell kiválasztani, hogy minden lehetséges problématípus megoldására megfelelő szakember álljon azonnal, vagy gyorsan behívható módon rendelkezésre.

Rendszeresen (időszakonként) végrehajtandó tevékenységek

Az üzemeltetésben résztvevő állomány rendszeresen (időszakonként) részesüljön oktatásban az üzemeltetési szabályzatról, amelynek keretében elemzik a korábban előfordult hibák, rendellenességek során szerzett tapasztalatokat és azok tanulságait.

A kormánybiztos a Kopint-Datorg Zrt. elnök-vezérigazgatóját jelölte ki, hogy a fentiekkel kapcsolatos intézkedések bevezetéséről és azok végrehajtásának folyamatos ellenőrzéséről gondoskodjon, és a tapasztalatokról rendszeresen tájékoztatást adjon.

1024 BUDAPEST, SZILÁGYI ERZSÉBET FASOR 11/B., TELEFON: 441-2583 FAX: 441-2502
E-MAIL: IBF@EKK.GOV.HU

3. esemény: Központi Rendszer azonosításkeveredése – 2009. február 7.

Az esemény rövid leírása

A Központi Rendszer 2009. január 20-i túlterhelés miatti lelassulása okainak elemzése során több olyan tényező került feltárásra, amely a rendszer teljesítményének nem optimális kihasználását mutatta. A rendszert üzemeltető Kopint-Datorg Zrt. fejlesztői az elemzések eredményeként olyan megoldásokat találtak, amellyel a rendszer teljesítményét – állításuk szerint – 2 nagyságrenddel sikerült megnövelni. A javítások belső tesztelése során rendellenességet nem tapasztaltak, és javasolták annak éles üzembe helyezését, amelyre 2009. február 7-én 8:33-kor, a rendszer leállítása nélkül sor került. **A MeH illetékes főosztályát a módosításnak az éles rendszerbe állításáról nem értesítették**.

A Központi Rendszer Helpdeskjéhez 12:06-kor érkezett bejelentés a Kormányzati Ügyféltájékoztató Központtól (KÜK), amely szerint több felhasználó jelezte, hogy saját adataival nem tud belépni az ügyfélkapun, viszont a bejelentkezési kísérlet eredményeként más felhasználó neve jelenik meg. A hibáról az első – interneten dokumentált – feljegyzés 10:27, az Aktafórum.hu könyvelői oldalon. A KÜK-től kapott tájékoztatás szerint kb. ettől az időponttól kezdődtek először szórványosan, majd egyre sűrűbben a bejelentések a hibáról. **Az érvényes eljárásrend szerint a KÜK abban az esetben értesíti hibabejelentésről a Központi Rendszer Helpdeskjét, ha a bejelentések száma 5 percen belül meghaladja a 10-et**.

A hiba ellenőrzését és behatárolását a Kopint-Datorg Alkalmazás Üzemeltetési Osztály ügyeletese azonnal megkezdte, és jelezte a hibát a Fejlesztési Osztály ügyeletesének. **Az ügyeletesek saját felhasználónevükkel történő bejelentkezése során a hiba egyikőjüknél sem jelentkezett.** Ennek ellenére a fejlesztési osztály ügyeletese javaslatára kiürítették a 2-es web-kiszolgáló átmeneti tárát, majd újraindították a web-szervereket, és visszaálltak a módosítás előtti állapotra.

Figyelembe véve, hogy további hibajelzések érkeztek, ezért következő lépésben mindkét web-kiszolgálón kiürítették az átmeneti tárat, és újraindítást hajtottak végre. Ezt követően **15:13-tól a hibajelzések megszűntek**.

A vizsgálat megállapításai

A vizsgálat megállapította, hogy az ügyfélkapu beléptetési moduljának átmeneti tárában (cache) keletkezett olyan üzemzavar, amely **az abban az időszakban belépett felhasználók egy része esetében a kapcsolatok keveredését okozta**. Megállapítást nyert, hogy a rendszer gyorsítása érdekében készített – a tesztrendszerben előzetesen hibátlanul működő – módosított program hibás konfigurációs beállítások miatt idézte elő a jelenséget. Az éles üzembe helyezés során néhány konfigurációs beállítás módosításra került, ugyanakkor az alapértelmezettől eltérő korábbi beállítások nem lettek ismételten megadva, aminek következtében azok alaphelyzetbe álltak. **A hibát sikerült reprodukálni, így egyértelműen bizonyítható, hogy az üzemzavart a hibás konfigurációs beállítás okozta.**

Megállapítást nyert, hogy **a hiba következtében a bejelentkező felhasználó véletlenszerűen (de nem minden esetben) egy – már bejelentkezve levő, vagy szintén éppen bejelentkezni**

szándékozó – másik felhasználónak az adataival lett beléptetve az Ügyfélkapu belső felületére. **Ha valaki nem volt bejelentkezve az adott időszakban az ügyfélkapura, annak semmilyen adatához nem lehetett hozzáférni! A fenti véletlenszerű eseten túl – célzottan – más felhasználó adataival történő belépés lehetősége nem állt fenn**. Az esetek egy részében minden továbblépés után más-más felhasználó neve jelent meg.

A Kürt Információbiztonsági és adatmentő Zrt. által elvégzett logelemzés megállapította, hogy 10.20-tól 15.13-ig nem teljeskörűen az összes belépett (21353) felhasználónál, hanem legfeljebb 129 felhasználó között véletlenszerűen összesen 832 esetben történt kapcsolati kód keveredése (a lognak ez az adata azt mutatja, hogy az érintett felhasználók hány alkalommal „kattintottak" más neve alatt). A 832 eset mintegy 90%-a az értesítési tárhely dokumentumainak a listáját érintette, azok kinyitására 100 alatti esetben került sor, és ezek közül is csak a visszaigazolások váltak olvashatóvá, a beküldött dokumentumok a titkosítás miatt más számára nem voltak értelmezhetők.

A hiba következtében (lehetséges, de nem feltétlenül megvalósított esetek):

- a felhasználó hozzáférhetett annak a másik felhasználónak a Központi Rendszer által biztosított tartós tárához, akinek a nevét a rendszer véletlenszerűen a sajátja helyett számára megjelentette,
- törölhette annak ügyfélkapus regisztrációját (18 ilyen esetre került sor),
- letölthette a más címére érkezett visszaigazolásokat, üzeneteket
- kitörölhette a másik felhasználó dokumentumait az átmeneti és a tartós tárból,
- módosíthatta az elektronikus levélcímet és az ügyfélkapu lejárati dátumát;
- **a tartós tárban elhelyezett, titkosító kulccsal ellátott dokumentumokat kimásolhatta, de azok tartalmához – a titkosító kulcs hiánya miatt – nem férhetett hozzá**.
- átmehetett valamely szakrendszer szolgáltatásaihoz (APEH, VPOP, OEP, ONYF, MVH, FELVI), és a szakrendszer által engedélyezett szolgáltatásokat igénybe vehette.

Ez utóbbi lehetőség az OEP, ONYF, FELVI és MVH rendszere esetében az adatokhoz történő hozzáférést nem tette lehetővé, tekintettel arra, hogy e rendszerek a saját rendszerbe belépéshez további azonosító adatot kérnek. A VPOP rendszere esetében – szombati nap lévén – minimális volt a forgalom (2 fő részéről), az ONYF felé átlépők száma 79 fő volt. Az APEH vizsgálja a szakrendszerébe az adott időszakban belépett mintegy 10000 felhasználó tranzakcióit. A Központi Rendszer üzemeltetőjének információi szerint **magánszemély adófolyószámláját ebben az időszakban 259 esetben kérdezték le**, ez a szám az összes lekérdezések száma, az a logokból – adatvédelmi okok miatt – nem állapítható meg, hogy ebből hány volt az illetéktelen (más adófolyószámlájához történő) hozzáférés.

A kapcsolatkeveredés során a leginkább érintett APEH rendszer ugyan ismételten nem végzi el a bejelentkező azonosítását, azonban dokumentumfeltöltés esetén ha a beküldő nem azonos, illetve nem meghatalmazottja a bevalláson szereplő személynek, akkor azt a dokumentumot a rendszer nem dolgozza fel, és erről értesítést küld mind a beküldőnek, mind a dokumentumon szereplő személynek. Ez alapján megállapítható, hogy **téves adatfeldolgozásra az APEH rendszerében nem került sor**.

Az APEH-nél végzett vizsgálat kitért arra is, hogy az érintett elektronikus bevallási (EBEV) fiókok esetében olvasás céljából kevesebb mint 80 felhasználói fiókhoz férhettek hozzá (a pontos szám megállapítása még folyamatban van). **A tételesen vizsgált esetekben adatmódosítás, jogosulatlan tevékenység nem történt, az esetek jelentős részében – a logok által igazolt adatok szerint – azonnal kiléptek a rendszerből. Célzott hozzáférés az**

APEH rendszere esetében sem volt lehetséges, adótitok szándékos megsértésére a hiba nem adott lehetőséget.

Figyelembe véve, hogy a hiba szombati napon jelentkezett, az érintettek száma a szokásos napi bejelentkezők számához viszonyítva alacsony volt, **08:33 és 15:13 között** (a hibát kiváltó módosítás végrehajtása és a hiba megszűnésének ideje alatt) **összesen 21353 felhasználó jelentkezett be** (csúcsidőszakban a bejelentkezők száma ezt 1 óra alatt meghaladja). **A hiba nem minden bejelentkező felhasználó esetében jelentkezett, de annak megállapítása, hogy pontosan hány felhasználót érintett – utólag már nem határozható meg, mivel az adatvédelmi követelmények szerint az azonosításhoz kapcsolódó információk nem tárolhatók.**

Az összes, 21353 érintettnek kiküldött levélre 29 esetben érkezett olyan visszajelzés, amely a hibás működésből eredő tevékenységre utal: regisztráció törlése, illetve az e-mail cím megváltoztatása. Ezek az adatok a jelzések alapján visszaállításra kerültek.

A vizsgálat módszertana

1. A vizsgálat minden lehetséges ok bekövetkezésének előfordulására kiterjedt. Ezek:
   a) esetleges külső támadás következménye;
   b) hibás alkalmazás (szkript), illetve konfigurálás éles rendszerbe állítása;
   c) átmeneti hardver meghibásodás;
   d) hibás üzemeltetői beavatkozás.

2. A vizsgálat kiterjedt az adatvédelmi és biztonsági szempontból lehetséges kockázati tényezőkre:
   a) a regisztrációs adatbázishoz történt-e hozzáférés?
   b) személyes adatokhoz történt-e hozzáférés?
   c) célzottan kiválasztható volt-e egy bizonyos felhasználó bejelentkezési adata?
   d) más szakrendszerekben történt-e (pl. adótitok körébe tartozó) adatokhoz hozzáférés?

3. A vizsgálat egyidejűleg kiterjedt az üzemeltetési szerződés, a hatályos szabályzatok és eljárásrendek betartására, valamint az üzemeltető Kopint-Datorg jelen levő szakembereinek tevékenységére is.

A vizsgálatba a Kopint-Datorg üzemeltetési és alkalmazásfejlesztési szakemberein, valamint az APEH informatikai biztonsági szakemberein kívül külső, független szakértők is bevonásra kerültek: a Kürt Információbiztonsági Zrt., amely korábban az ügyfélkapu minőségbiztosítási feladatait is ellátta, valamint több fejlesztő és informatikai biztonsággal foglalkozó céggel is konzultációkra került sor. Minden szükséges segítséget felajánlott a Nemzetbiztonsági Hivatal, valamint a CERT-Hungary Központ, amelyek igénybe vételére – tekintettel arra, hogy nem hacker-támadás következett be, nem került sor.

Megállapítások

1. a) Megállapítást nyert, hogy a **külső támadás lehetősége** az Aktív Védelmi Rendszer logjai és információi alapján **teljes mértékben kizárható**. Sem DoS támadást, sem behatolást az AVR nem detektált. Az érintett 4 szolgáltatási pont esetében az adott időszakban összesen 1

darab alacsony súlyosságú (kivédett) támadás volt 14:27:47-kor, amely az esemény szempontjából nem releváns.

Az EKG hálózati betörés érzékelési rendszere által a kérdéses időszakban, az ügyfélkapu infrastruktúra front oldali szolgáltatási pontjaira vonatkozóan detektált események **elsődleges elemzése** alapján az érzékelt jelek nem utalnak az Ügyfélkapu rendszer elleni célzott hálózati támadásra.

b) A Központi Rendszer 2009. január 20-i túlterhelés miatti lelassulása okainak elemzése során feltárt gyorsítási lehetőségek kihasználására a Kopint-Datorg fejlesztői konfiguráció módosítást végző szkriptet írtak, amely a rendszer teljesítményét – a tesztrendszeren végzett mérések szerint nagyságrendekkel javíthatta. A vizsgálat többszöri ellenőrzés után megállapította, hogy a konfiguráción végzett módosítás önmagában nem volt hibás, az – a korábbi, az alapértelmezettől eltérő, konfigurációs beállításokkal együtt – valóban a rendszer gyorsulását eredményezte volna. **A hibajelenséget ugyanakkor kétséget kizáróan, és reprodukált módon az okozta, hogy a konfigurációs módosítás során az alapértelmezettől eltérő beállítások nem lettek érvényesítve, és azok az eredeti értékükre álltak vissza.**

c) Az átmeneti hardver hiba bekövetkezésének lehetőségét a Kürt Zrt. a logok elemzése révén vizsgálta, és azt egyértelműen kizárta. A logelemzés keretében a Kürt Zrt. a január 20-i rendszerlassulás vizsgálatát is végezte, és feltárt néhány, a rendszerben levő szűk keresztmetszetet.

d) A hibás üzemeltetői beavatkozás keretében az üzemeltető Kopint Datorg részéről az adott időszakban ügyeletben levő és berendelt munkatársak tevékenysége került szinte percenkénti pontossággal elemzésre.

Megállapítható, hogy az ügyeletben levő munkatársak **a *hibabejelentés fogadásától annak elhárításáig* a szakmai tevékenységük során az üzemeltetési szabályzat szerint jártak el**. **Ugyanakkor az is megállapítható, hogy a módosítás éles rendszerbe töltése előtt, valamint annak megvalósítása során eljárásrendi szabályokat sértettek meg**, illetve megsértették az üzemeltetési szerződés azon pontját, amely szerint a változásról a Megrendelő (Miniszterelnöki Hivatal) képviselőjét/kapcsolattartót tájékoztatni szükséges. Ugyancsak megsértették a szerződés azon pontját, amely szerint a hiba okáról a Megrendelő kapcsolattartóját tájékoztatni szükséges, illetve a hiba bekövetkeztéről – egy megadott lista szerint – az érintetteket sms-ben tájékoztatni szükséges. Az eljárásrendi szabályok megsértésének pontos ismertetése a 3. pontban történik.

2. a) A vizsgálat során a logok elemzése alapján megállapítást nyert, hogy **az ügyfélkapu felhasználóinak adatait tartalmazó regisztrációs adatbázishoz senki nem fért hozzá, a felhasználói bejelentkezéshez szükséges információ nem került ki a rendszerből.**

b) **A személyes adatok körébe tartozó információkhoz a hozzáférés lehetősége** – arra a személyre vonatkozóan, akinek a nevében a véletlenszerű belépés történt – **fennállt**. A Központi Rendszer esetében csak a név, anyja neve, születési hely, születési idő, és a regisztrációkor megadott e-mail címre megismerésére nyílt lehetőség. A tartós tárban vagy az értesítési tárhelyen levő – titkosító kulccsal nem ellátott – dokumentumokban szerepelhetett a felhasználó neve, címe és adóazonosító száma, vállalkozások esetében a cégadatok

nyilvánosan – a cégnyilvántartásban is elérhető adatok. Azt, hogy hány alkalommal történt ilyen dokumentum kinyitása és elolvasása, nem megállapítható. Ez adatvédelmi okokból nem kerül naplózásra.

c) **Megállapítást nyert, hogy célzottan – egy meghatározott felhasználó – nevében a bejelentkezés nem volt lehetséges**. A belépő felhasználó nevétől eltérő nevet a rendszer az érintett 129 felhasználó esetében egymás közül véletlenszerűen adta ki.

d) A más szakrendszerek adataihoz történő hozzáférés körében az APEH rendszerébe történt belépések esetén kerülhetett sor adótitok körébe tartozó információk megismerésére. Ennek mértékét az APEH vizsgálja. Az előzetes információk szerint az adott időszakban az APEH rendszerébe mintegy 10000 belépés történt, ebből 259 esetben került lekérdezésre magánszemély adófolyószámla adata. **Az adófolyószámlák adatait csak lekérdezni lehetett, változtatni nem!**

A kapcsolatkeveredés során a leginkább érintett APEH rendszer ugyan ismételten nem végzi el a bejelentkező azonosítását, azonban dokumentumfeltöltés esetén ha a beküldő nem azonos, illetve nem meghatalmazottja a bevalláson szereplő személynek, akkor azt a dokumentumot a rendszer nem dolgozza fel, és erről értesítést küld mind a beküldőnek, mind a dokumentumon szereplő személynek. Ez alapján megállapítható, hogy **téves adatfeldolgozásra az APEH rendszerében nem került sor**.

A tételesen vizsgált esetekben adatmódosítás, jogosulatlan tevékenység nem történt, az esetek jelentős részében – a logok által igazolt adatok szerint – azonnal kiléptek a rendszerből. **Célzott hozzáférés az APEH rendszere esetében sem volt lehetséges, adótitok szándékos megsértésére a hiba nem adott lehetőséget**.

3. A vizsgálat kiterjedt a hatályos jogszabályok, szabályzatok és eljárásrendek, valamint az üzemeltetési szerződés betartására.

A Központi Rendszer működtetőjénél és üzemeltetőjénél 2008. szeptember 1-10. között az informatikai biztonsági felügyelő célellenőrzést hajtott végre. A vizsgálat összegzett megállapítása szerint:

„*A jelenlegi technológiai megoldásában 2005. május 1. óta működő (és folyamatosan bővülő szolgáltatásokat biztosító) Központi Rendszer eddigi működtetése során* ***informatikai biztonsági hiányosságokra visszavezethető adatszivárgás, adatvesztés, illetve kockázati tényezőként értékelhető sikeres behatolás nem fordult elő****. Mindez a kifejlesztett rendszer informatikai biztonsági szempontból hatékony technikai megoldásainak, és az üzemeltetés magas szintű ellátásának érdeme.*

Az ellenőrzés során feltárt hiányosságok többségében formai jellegűek, amelyek pótlása, illetve korrigálása a rendszer még magasabb szintű biztonsága érdekében szükségesek. ***A hiányzó (illetve hiányos) eljárásrendek pótlása az esetlegesen bekövetkező váratlan helyzetekben az üzemmenet folytonosságát vagy a károk enyhítését biztosító szakszerű és tudatos tevékenységek érdekében kiemelt fontosságúak***.”

A Központi Rendszer Informatikai Biztonsági Szabályzata és Üzemeltetési Szabályzata a célellenőrzés jegyzőkönyve szerint a kisebb – korrigálásra szoruló – eljárásrendi és formai hiányosságok ellenére megfelelő, és alkalmas a Rendszer biztonságos üzemeltetésére.

A február 7-i esemény kapcsán:

a) Megállapítást nyert, hogy az esemény *A Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről* szóló **84/2007. (IV. 25.) Korm. rendelet 6§ (1) pontjában érintett felelősség körébe tartozik**: „***Az üzemeltető szervezet felelős a Központi Rendszer általa üzemeltetett alrendszereinek biztonságáért, és tevékenységével nem veszélyeztetheti a Központi Rendszer más elemeinek biztonságát***."

b) Megállapítást nyert, hogy a felelősség kérdésében A központi elektronikus szolgáltató rendszerről szóló 182/2007. (VII. 10.) Korm. rendelet több pontja is rendelkezik:

- 13. § (2) „*A csatlakozási megállapodás alapján* ***a kormányzati portál üzemeltetője biztosítja*** *az elektronikus szolgáltatás folyamatos, havi szinten legalább 99,5%-os szintű elérhetőségét a kormányzati portálon,* ***az elektronikus szolgáltatás személyazonosítást igénylő elemeinek működőképességét az ügyfélkapun keresztül****, valamint az elektronikus szolgáltatás ügyfélszolgálati támogatását a kormányzati ügyfél-tájékoztató központon keresztül*."
- 25. § (1) „*Az ügyfélkapu biztosítja, hogy az ügyfél egyedileg azonosított módon biztonságosan léphessen kapcsolatba a központi rendszer útján az elektronikus ügyintézést, illetve elektronikus szolgáltatást nyújtó szervezetekkel*.
  (2) *A* ***központi rendszer üzemeltetője olyan zárt rendszert tart fenn, amely biztosítja, hogy a központi rendszeren keresztül továbbított információkhoz csak az ügyfél, illetőleg a címzett férhet hozzá és azok védett részét az üzemeltető sem ismerheti meg.***"

c) Megállapítást nyert, hogy az esemény a 84/2007. (IV. 25.) Korm. rendelet 2. melléklet 3.17.1 pontja szerinti II. kategóriájú biztonsági esemény körébe sorolható, mellyel összefüggésben nem került végrehajtásra a 6. § (6) pont szerinti értesítés: „*Az üzemeltető szervezet a 2. melléklet 3.17.1 pontja szerinti I. és II. kategóriájú biztonsági esemény esetén* ***haladéktalanul jelentést tesz az informatikai biztonsági felügyelőnek.***"

d) Megállapítást nyert, hogy tesztelési terv nem készült, ezzel

- a módosítás tesztelése során **megsértették a Központi Rendszer Tesztelési Szabályzat 5.§ (1) pontját**, amely szerint „*A 2.§. (1) c) pontban meghatározott tesztelési tevékenységeket meg kell tervezni, a tesztelési tervet írásba kell foglalni*." (A 2.§ (1) c) pont: „*E szabályzat hatálya kiterjed: mindazokra a tevékenységekre és munkafolyamatokra, melyek a KR eszközkészletét bármilyen módon megváltoztatják, különösen új KR szoftver verziók bevezetése, új KR szoftver komponensek üzembe helyezése*".
- **megsértették a Tesztelési Szabályzat 5.§ (4) pontját:** „*Standard szoftverekre (operációs rendszer, adatbázis kezelő, egyéb szerver szoftver) vonatkozóan eseti teszt terveket kell kialakítani. Új szoftver komponens bevezetése esetén az igénybe vett funkcionalitásra, új verzió bevezetése esetén a változó funkcionalitásra tekintettel kell kidolgoznia a tesztelési tervet. E feladat felelőse az IT1 Osztály*."
- éles környezetben teszt futtatására nem került sor, ezzel különösen **megsértették a Tesztelési Szabályzat 5.§ (6) pontját** „*A teszt tervnek elkülönítetten kell meghatároznia a*

KR teszt és éles környezetben végrehajtandó tesztelési tevékenységeket. A KR éles környezetben végrehajtandó tesztelésnek tükröznie kell a két környezet különbségeiből adódó eltéréseket. Az éles környezetben végrehajtandó tesztnek e különbségekre kell koncentrálnia."

e) Megállapítást nyert, hogy az üzembe helyezésről a Működtető (MeH) felelős (kapcsolattartó) munkatársának döntését nem kérték ki, ezzel **megsértették a Tesztelési Szabályzat 9.§ (5) pontját: „***Új KR szoftver komponens tesztelési folyamatának lezárásakor az ÜÜ vezetőjének javaslata alapján a Működtető dönt az üzembe helyezésről*."

A változásról nem értesítették a Működtetőt (kapcsolattartót), aki a hiba jelentkezésekor az információ hiányában nem tudott azonnali döntést hozni, figyelembe véve, hogy a változásról nem volt tudomása. Ezzel **megsértették a Tesztelési Szabályzat 9.§ (6) pontját: „***Minden jóváhagyott szoftverváltoztatásról – függetlenül a jóváhagyó személyétől – haladéktalanul értesíteni kell a Működtetőt.*" Ezzel nem teljesítették a Vállalkozói Szerződés Melléklete 10. oldalán „A vállalkozó hibabejelentéssel kapcsolatos feladatai alatt" menüben lévő 1. pontot, mert a Működtetőt (kapcsolattartó) nem kapta meg a hiba okát.

f) A Központi Rendszer Változáskezelési Szabályzatának 3.§-a meghatározza a „Változás", valamint a „Változás kategória fogalmát".

- a fentiek alapján **megsértették a Változáskezelési Szabályzat 4.§ (3) pontját**: „*Taktikai változásra vonatkozó döntést is kizárólag Működtető hozhat az Üzemeltető vagy tanácsadó javaslatára*"
- tekintettel arra**,** hogy a változás a Működtető (kapcsolattartó) által nem lett jóváhagyva, **megsértették a Változáskezelési Szabályzat 7.§ (1) pontját:** „*Stratégiai, taktikai és mennyiségi változás esetén a változás jóváhagyása a KR Tesztelési szabályzatában leírt módon történhet. A jóváhagyást és a kezdeményezését az Üzemeltető írásba foglalja*."

g) Az **Üzemeltető nem teljesítette** a Vállalkozói Szerződés Melléklete 10. oldalán „A vállalkozó **hibabejelentéssel kapcsolatos feladatai** alatt" menüben lévő 2. pont szerinti kötelezettségét, miszerint 20 percen belül mindenkit tájékoztatnia kellett volna a hibáról, amely nem történt meg.

h) A működést befolyásoló tényezőkről az **Üzemeltető elmulasztotta a 182/2007. Korm. rendelet** 40. § (3) pontja szerinti értesítési kötelezettség teljesítését: „*A (2) bekezdésben foglaltakkal egy időben, a központi rendszer üzemeltetője értesíti a központi rendszer által a csatlakozott szervezetek számára nyújtott szolgáltatások üzemzavarában érintett közvetített elektronikus szolgáltatásokat nyújtó, csatlakozott szervezeteket az üzemzavar tényéről, illetve annak megszűnéséről*, valamint **az EKG üzemeltetési szerződés 4.1 szerinti folyamatos tájékoztatás**, valamint a Szerződés mellékletét képező „Szolgáltatás-leírás" 2.4 pontja szerinti tájékoztatási **kötelezettségét**.

A fentiek alapján az Üzemeltető részéről a Központi Rendszerre vonatkozó hatályos jogszabályok, szabályzatok, valamint az üzemeltetéssel kapcsolatos vállalkozási szerződés egyes pontjainak sorozatos megsértése állapítható meg. **Bár a hibát közvetlenül kiváltó konfiguráció-módosítás hibája közvetlenül – jelen állás szerint – nem volt megállapítható, a hatályos szabályzatok és eljárásrendek sorozatos megsértése miatt bekövetkezett erkölcsi kár az Üzemeltető felelőssége**.

A vizsgálat lezárult, a hiba pontos oka behatárolásra és reprodukálásra került. **Az esemény ugyanazokra az okokra vezethetők vissza, mint a 2009. január 20-i rendszerlassulás**. A január 20-i eseménnyel kapcsolatban az infokommunikációért felelős kormánybiztos által tett, és a Kopint-Datorg Zrt. vezetése számára javasolt intézkedések erre az eseményre is érvényesek.

Kiegészítő intézkedésként azonnali hatállyal bevezetésre került, hogy a Központi Rendszert érintő súlyos rendszerhiba észlelése, vagy az erről szóló hibabejelentés érkezése esetén a KÜK azonnal értesíti a Központi Rendszer Helpdeskjét, amely „sárga riasztást" rendel el, és megkezdi a hiba ellenőrzését; ismételt hibabejelentés esetén „piros riasztás" keretében – **amennyiben a hiba a rendszer biztonságát vagy az adatbiztonságot veszélyezteti – az üzemeltető saját hatáskörben dönthet a rendszer azonnali leállításáról**.

Összegzett megállapítások a három eseménnyel kapcsolatban

A működési zavarok mindhárom esetben ugyanarra az okra vezethetők vissza: emberi mulasztásra, a programok módosítását követő, nem az erre vonatkozó hatályos szabályzatok előírásainak megfelelő és nem körültekintően végzett tesztelésre. Az esetek – az érintett felhasználóknak okozott kellemetlenségen kívül, amelyért mind az OEP, mind a MeH az érintettektől elnézést kért – adatvesztést, visszaállíthatatlan adatmódosulást, anyagi kárt nem okoztak. **A rendszerek biztonságát, az adatok közhitelességét az üzemzavarok nem veszélyeztették.**

A hibás működés okai, és a felelősök mindhárom esetben egyértelműen megállapítást nyertek, a felelősségre vonások folyamatban vannak.

Az események miatt mind az OEP-nél, mind a Központi Rendszert működtető Miniszterelnöki Hivatalnál intézkedési terv készült a hasonló esetek bekövetkezésének megakadályozására. Az eseményekről az informatikai biztonsági felügyelő részletes jelentést készített.

A Központi Rendszer esetében megállapítható, hogy a rendszer az adóbevallási határnapokon csak a gyorsított dokumentumfeltöltési üzemmódban képes a megnövekedett igényeket kiszolgálni, amely időszakban a kormányzati portál többi szolgáltatása nem elérhető. **A kapacitások növelése érdekében – figyelembe véve a tervezett további szolgáltatások indítását is – elengedhetetlen a szolgáltatás rekonstrukciója és áteresztő képességének növelése, amelyre az Ügyfélkapu-2 projekt keretében 2009. december 1-ig kerül sor.**

Az eseményekből leszűrhető tanulságok rámutatnak arra, hogy az informatikai biztonság körébe tartozó üzemmenet-folytonosság biztosítása már nemcsak megfelelő tűzfalak és vírusvédelmi rendszer beállítását jelenti, hanem az üzemeltetés teljes folyamatára ki kell terjedjen, amely az informatikusok részéről a korábbinál jóval nagyobb odafigyelést, a szabályzatok, eljárásrendek pontos betartását és a módosítások körültekintő éles üzembe helyezését igényli. Hasonló esetek korábban is sok helyen előfordultak, azonban a kisebb – „házon belüli" – rendszerek esetében ezek nem jártak különösebb következménnyel.

A lakosság széles körét érintő, és személyes adatait kezelő országos rendszerek, közhiteles nyilvántartások esetében az informatikai rendszerek fejlesztésének és üzemeltetésének a korábbiaknál magasabb követelményeknek kell megfelelniük. Ehhez járulhat hozzá **az elektronikus szolgáltatások informatikai biztonsági auditjának kötelezővé tétele a kritikus infrastruktúrák és az elektronikus közigazgatási szolgáltatások esetében**. Az erre vonatkozó rendelkezést az előkészítés alatt álló informatikai biztonságról szóló törvény-javaslat tartalmazza.

Budapest, 2009. február 24.

Dr. Dedinszky Ferenc

1024 BUDAPEST, SZILÁGYI ERZSÉBET FASOR 11/B., TELEFON: 441-2583 FAX: 441-2502
E-MAIL: IBF@EKK.GOV.HU