A Kormány

…/2013. (……) rendelete
a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról, illetve az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről szóló 212/2010. (VII. 1.) Korm. rendelet módosításáról

A Kormány az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24.§ (1) a)-d) pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. §

E rendelet alkalmazásában
1. adminisztrátori jogosultsággal rendelkező vizsgálat: a biztonsági vizsgálati eljárás során a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, az eljárás célja, hogy megfelelőségi listák alapján a teljes informatikai rendszer állapota ellenőrzésre kerüljön;
2. automatizált vizsgálat: a biztonsági vizsgálati eljárás során a szervezet informatikai rendszerének a sérülékenységei célszoftverek segítségével kerülnek feltérképezésre;
3. belső vizsgálat: a biztonsági vizsgálati eljárás során a szervezet informatikai rendszerének sérülékenység vizsgálata a belső hálózati végpontról közvetlenül történik;
4. biztonsági besorolás: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) szerinti az elektronikus információs rendszerek biztonsági osztályba és a szervezet biztonsági szintbe sorolás együttese;
5. célszoftverek: a biztonsági vizsgálati eljárás során a sérülékenység-vizsgálat egyes fázisainak végrehajtására kifejlesztett szoftverek;
7. hálózati végpont: adott informatikai rendszer hálózatához való csatlakozási pont;
9. regisztrált felhasználói jogosultság nélküli vizsgálat: a biztonsági vizsgálati eljárás során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik a szervezet informatikai rendszeréről, illetve nincs felhasználói jogosultsága a rendszerhez;
10. kézi vizsgálat: a biztonsági vizsgálati eljárás során a szervezet informatikai rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre;
11. külső vizsgálat: az informatikai rendszer internet felőli, külső sérülékenység-vizsgálata, mely során az interneten fellelhető, publikus adatbázisokban való szabad keresés, célzott információgyűjtés, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerül sor;
12. emberi tényezőkön alapuló vizsgálat: a dolgozók általános informatikai felkészültségének, és a szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.
13. Nemzeti Tanúsítási Rendszer: a „Common Criteria for Information Technology Security Evaluation” nemzetközi információ technológiai biztonsági értékelési szabványrendszernek megfelelő, valamint az elektronikus információs rendszer logikai, fizikai és adminisztratív védelmi intézkedései megfelelőségének értékelésre elfogadott magyar tanúsítási séma;

14. regisztrált felhasználói jogosultsággal rendelkező vizsgálat: a biztonsági vizsgálati eljárás során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot;
15. sérülékenység-vizsgálat: a biztonsági vizsgálati eljárás során meghatározott módszertan alapján különböző fázisokban (jogosultság, irányultság alapján) a szervezet teljes információs rendszerének sebezhető pontjai, hiányosságai, hibás konfigurációs beállításai kerülnek feltárásra, továbbá a feltárt hiányosságok elhárítására vonatkozó intézkedési terv kerül megfogalmazásra;
16. Tanúsító Szervezet: a Nemzeti Tanúsítási Rendszer keretében tanúsítási eljárásokra jogosult szervezet.
17. titkosítási eljárás: olyan eljárás, mely az adat megismerhetőségét azáltal korlátozza, hogy az adat egy algoritmus segítségével átalakításra kerül olyan karaktersorozattá, ami olvashatatlan olyan személy számára, aki nem rendelkezik a visszaalakításhoz szükséges egyedi karaktersorozatból álló kulccsal;
18. titkosítási kulcsok: titkosítási eljárás során alkalmazott olyan karaktersorozatok, melyek ismeretében a titkosított állomány megismerhető;
19. webes vizsgálat: a biztonsági vizsgálati eljárás során automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások jól ismert, illetve a nem dokumentált sérülékenységei;
20. Vizsgáló Szervezet: az a jogi személy, aki a termék és elektronikus információs rendszerértékeléseket végzi a magyar tanúsítási séma alapján.
21. wifi vizsgálat: a biztonsági vizsgálati eljárás során a hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik;
22. 3G/GPRS vizsgálat: 3G/GPRS/ szolgáltatások sérülékenység-vizsgálata, melynek során a hálózatok és az elérhető szolgáltatások automatizált és kézi vizsgálati módszerrel történő feltárására kerül sor;

2.§

Általános rendelkezések

(1) A Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: hatóság) az elektronikus információs rendszerek tekintetében ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.) meghatározott elektronikus információbiztonsággal kapcsolatos hatósági, illetve a jogszabályban meghatározott egyéb feladatokat. A hatóság az érintett szervekkel kapcsolatos tevékenysége során az Ibtv. 6. §-ában foglaltak érvényesülése érdekében jár el.

(2) A hatóság vezetőjét az informatikáért felelős miniszter (továbbiakban miniszter) nevezi ki határozatlan időre. A hatóság elnökének az a kormánytisztviselő nevezhető ki, aki rendelkezik legalább öt év vezetői gyakorlattal – amelynek időtartamába beleszámítható minden olyan közigazgatáson kívüli vezetői gyakorlat is, amelyet a tisztviselő egyéb munkavégzésre irányuló jogviszonyalapján látott el – illetve nem tagja olyan vállalkozásnak, amely információ technológiai tevékenységet folytat.

(3) A hatóság eljárásainak ügyintézési határideje hatvan nap, amelyet a hatóság vezetője indokolt esetben egy alkalommal, legfeljebb harminc nappal meghosszabbíthatja.

(4) A hatóság eljárását kérelemre, vagy hivatalból folytatja le. Hivatalból folytatja le az eljárását, ha
a) az ellenőrzési terv alapján,
b) az általa végzett kockázatelemzés, ellenőrzés, valamint az Ibtv. hatálya alá tartozó szerv, szervezet, vagy személy (továbbiakban: érintett szerv) által a jogszabály alapján kötelezően szolgáltatott adatok, vagy a szakhatóság, a kormányzati, vagy ágazati eseménykezelő központ(ok), illetve más hatóság jelzése alapján
információ biztonságot veszélyeztető hiányosságot, mulasztást észlel, illetve a biztonsági követelmények megsértését állapítja meg. A hatóság az eljárás megindítása előtt jogosult tájékoztatást kérni az érintett szervtől az információbiztonsági követelmények betartásáról.

(5) A hatóság az eljárását lezáró döntése meghozatala előtt az érintett szervvel – amennyiben ezt azonnali fenyegetés vagy biztonsági esemény, illetve az érintett szerv ismételt jogsértő magatartása nem zárja ki – egyeztetést folytathat le, amelybe szükség szerint a szakhatóságot, a kormányzati, illetve ágazati eseménykezelő központokat bevonja.

(6) A hatóság eljárása során jogosult
a) bármely eszközt, iratot, dokumentumot megtekinteni, megvizsgálni, azokról másolatot, kivonatot készíteni,
b) az érintett szerv vezetőjét, vagy a szervezet nevében nyilatkozni jogosult egyéb személyt, továbbá annak alkalmazottait, a biztonságért felelős személyt, az érintett szerv által az adatkezeléshez, adatfeldolgozáshoz igénybevett közreműködőt, vagy az érintett szerv elektronikus informatikai rendszerének üzemeltetőjét szóban vagy írásban adatszolgáltatásra, illetve egyéb felvilágosítás adására kötelezni.

(7)Amennyiben a jogkövetkezményekre való figyelmeztetés ellenére az érintett szerv az eljárás során nem működik együtt a hatósággal, a hatóság a fokozatosság elvének figyelembe vételével az Ibtv. 16-17. §-a szerinti bármely szankciókat alkalmazhatja, figyelemmel arra, hogy az érintett szerv költségvetési szervnek minősül, vagy sem.

(8) A hatóság eljárása során az Ibtv-ben meghatározott feladatai ellátása érdekében – az intézkedéssel érintett működésének és ügyvitelének lehető legkisebb mértékű zavarása vagy akadályozása mellett – helyszíni ellenőrzés keretében jogosult önállóan, vagy a szakhatósággal, illetve más hatósággal együtt is:
a) az érintett szerv információ technológiai tevékenységével összefüggő helyiségeibe belépni,
b) az érintett szerv számára adatfeldolgozást, adatkezelést biztosító, illetve információ technológiai szempontból érintett helyszínein ellenőrzést tartani, és ennek során bármely, az elektronikus információbiztonsággal kapcsolatos okiratot, dokumentumot, szerződést, aktív, vagy passzív eszközt, információs rendszert, biztonsági intézkedést megismerni, ellenőrizni,
c) információ technológiai műszaki vizsgálatokat végezni.

(9) A tényállás tisztázása során a hatóság egyebekben a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (továbbiakban: Ket.) tényállás tisztázására és a hatósági ellenőrzésre vonatkozó szabályait is alkalmazza.

(10) A hatóság vezetője a helyszíni ellenőrzés elrendelése esetén a hatóság ellenőrzést ellátó munkatársa részére megbízólevelet állít ki. A megbízólevélnek tartalmaznia kell az ellenőrzés célját, tárgyát, az elrendelésre okot adó körülményeket, illetve jogszabályi hivatkozást, az ellenőrzés várható időtartamát, az ellenőrzés módját és az ellenőrzést végző személyek megnevezését.

(11) A helyszíni ellenőrzés elrendeléséről az érintett szerv vezetőjét előzetesen, a helyszíni vizsgálat megkezdése előtt legalább 5 nappal korábban, írásban értesíteni kell. Az értesítés mellőzhető, ha
a) súlyos fenyegetettség áll fenn,
b) súlyos biztonsági esemény történt,
c) az a)-b) pontok bekövetkezése valószínűsíthető,
d) az a helyszíni ellenőrzés eredményes lefolytatását a rendelkezésre álló adatok alapján várhatóan meghiúsítaná.

(12) A hatóság helyszíni ellenőrzést végző munkatársa az adott helyszínen érvényes munkavédelmi, vagy más biztonsági rendszabályt köteles betartani. Az ellenőrzéssel érintett szerv vezetője, minden – ideértve az Ibtv. 2. § a) és b) pontja szerinti szerveket és személyeket – munkatársa, illetve a biztonságért felelős személy az Ibtv. 12.§ c) pontja alapján köteles a hatósággal együttműködni.

(13) A helyszíni ellenőrzésről a hatóság jegyzőkönyvet készít, amelyet az ellenőrzés lezárását követő nyolc napon belül az érintett szervnek írásban észrevételezésre meg kell küldeni. Az érintett szerv azzal kapcsolatban nyolc napon belül írásban tehet – a hatóságot nem kötelező – észrevételeket. Az észrevételek tisztázása érdekében a hatóság egyeztetést kezdeményezhet az érintett szervvel.

(14) A hatóság jogosult bármely, jogszabályban meghatározott eljárási cselekményt soron kívül – szükség esetén a szakhatóság, a kormányzati és ágazati eseménykezelő központ, illetve az európai és nemzeti létfontosságú rendszerelemek nyilvántartására és a nyilvántartás adatainak kezelésére kijelölt szerv bevonásával – lefolytatni, ha az a magyar kiberteret, a nemzeti elektronikus adatvagyont, az állam és polgárai számára kiemelten fontos információs rendszereket súlyosan veszélyeztető fenyegetés elhárítását szolgálja.

(15) A hatóság – tekintettel az információ technológia folyamatos fejlődésére – jogosult ajánlás jelleggel állásfoglalások és tájékoztatók kibocsátására, amelyek betartásával az érintett szervek a védelmi felkészültségüket növelni képesek. Az állásfoglalások és tájékoztatók – amennyiben azokat biztonsági esemény megelőzése, fenyegetés elhárítása érdekében adta ki a hatóság – a hatósági ellenőrzés szempontjai közé beépülnek.

(16) A hatóság meghatározza azon eljárások körét, amelyben kötelező vagy kizárólagos az elektronikus kapcsolattartás. Elektronikus kapcsolattartás esetén az érintett szerv a bejelentéseit a hatóság által rendszeresített és az elektronikus közzététel szabályai szerint közzétett elektronikus űrlapon köteles benyújtani.

3. §

A hatóság feladatai

A hatóság az elektronikus információs rendszerek biztonsági felügyelete körébe tartozó feladatokon túl az alábbiakat látja el.

I. Európai Unió tagállamaiban történő adatfeldolgozás

(1) A hatóság az Ibtv. 3. § (2)-(3) bekezdése szerint üzemeltetett információs rendszerek tekintetében engedélyezési eljárást folytat le.

(2) Az engedélyezési eljárás kérelemre indul. Az eljárás során a hatóság megvizsgálja
a) a külföldön történő adatkezelés indokát,
b) a külföldön kezelt adatok és adatbázisok leírását,
c) hogy az adatkezelő rendszer valamint üzemeltetője nevesített-e, és az adatkezelés jogszabályi megfeleléséért felelős személy, vagy személyek neve, beosztása, elérhetősége ismert-e,
e) az adatkezelő rendszer technikai és technológiai – ideértve a hardver és szoftverkomponenseket is – leírását,
f) az adatkezelő rendszer információ biztonságának ismertetését, a rendszerhez kapcsolódó, illetve az üzemeltetőre vonatkozó belső szabályozásokat és utasításokat,
g) a kötelezően lefolytatandó biztonsági audit eredményét, valamint
h) a magyar információvédelmi szabályok megtartásáról szóló üzemeltetői nyilatkozatot.

(3) Nem kell a (2) bekezdés e) - g) pontok szerinti leírásokat megvizsgálni amennyiben az Ibtv. 4. §-a szerinti, érvényes biztonsági tanúsítvány a kérelem benyújtásakor rendelkezésre áll, és azt a hatóságnak bemutatják.

(4) A (2) bekezdés b) és e)-f) pontjai, illetve (3) bekezdés szerinti dokumentációkat, okiratokat az eredetivel megegyező másolatban, illetve hiteles magyar fordításban kell a kérelem mellékleteként benyújtani.

(5) A kérelem tartalmazza (2) és (3) pontok szerinti adatokat, és azt a külföldön történő adatkezelés megkezdését megelőzően be kell nyújtani.

(6) Engedély hiányában a tevékenység nem kezdhető meg. A kérelemben foglalt adatok biztonsági szempontokra kiható változásáról a hatóságot tájékoztatni kell. Az engedély lejártát a benyújtott tanúsítványok érvényességi időtartamára lehet megállapítani.

II. Európai Unió tagállamain kívül történő adatfeldolgozás

(7) Amennyiben az érintett szerv az adatkezelést, illetve üzemeltetést az Európai Unión kívül – ideértve a nem azonosítható adatkezelési, vagy jogszabály által kizárt helyszínen megvalósuló, úgy nevezett „felhő” szolgáltatásokat – folytatja, vagy kívánja folytatni, azt a hatóság felé a (2) bekezdés szerinti adattartalommal soron kívül be kell jelentenie.

(8) Amennyiben a hatóság tudomására jut a (7) bekezdés szerinti adatkezelés, illetve üzemeltetés, az érintett szervet a jogkövetkezmények kilátásba helyezésével soron kívül adatközlésre kötelezi.

(9) Az Ibtv. 3. §-ára tekintettel a (7) bekezdés szerinti tevékenység nem engedélyezhető. A hatóság az érintett szervet kötelezi az ilyen adatkezelés megszüntetésére, illetve arra, hogy soron kívül jelentse be mindazon intézkedéseket, amelyek biztosítják, hogy az adatok a későbbiekben sem juthatnak illetéktelenek tudomására.

(10) Amennyiben a külföldön végzett adatkezelésre nemzetközi szerződés alapján kerül sor, a hatóságot tájékoztatni kell az érintett adatokról, az adatfeldolgozó személyéről, és a szerződéses jogviszony tartalmáról. A hatóság a tájékoztatást tudomásul veszi.

III. Információ technológiai fejlesztési projektek ellenőrzése

(11) A központi, valamint az európai uniós forrásból megvalósuló fejlesztési projektek információbiztonsági követelményeinek teljesítése során a projekt vezetése a projekt tervezési szakában a hatóság rendelkezésére bocsátja mindazon dokumentációkat, amelyek alapján a biztonsági, és termékminősítési követelmények megvalósulása ellenőrizhető a projekt teljes életciklusában ideértve az átvétel (teljesülés) után a rendszer használata során érvényesítendő elvárásokat is.

(12) A dokumentációt olyan időben kell a hatóság rendelkezésére bocsátani, hogy annak észrevételei, vagy kifogásai a projekt terveken, illetve a projekt tárgyán átvezethető és alkalmazható legyen. A késedelemből adódó kockázatokat (ideértve a költségek viselését is) a projekt kivitelezéséért felelős viseli.

IV. A biztonsági besorolás ellenőrzése

(13) A biztonsági besorolás ellenőrzése a hatóságnak megküldött információk alapján történik.

(14) Amennyiben a bejelentett biztonsági besorolásokat – ideértve az Ibtv. 8. § (5) és 10. § (7) bekezdései szerinti cselekvési tervet is – a hatóság elfogadja, arról külön döntést nem hoz. Az elfogadást megtörténtnek kell tekinteni, amennyiben a hatóság 30 napon belül más döntéséről az érintett szerv vezetőjét nem értesíti. Az elfogadás a biztonsági besorolások későbbi önálló, vagy az érintett szerv ellenőrzése során történő felülvizsgálatát nem zárja ki.

(15) Amennyiben a hatóság az eljárása során az érintett szerv által megállapított biztonsági besorolási szintnél magasabb biztonsági besorolási szintet állapít meg, arról kötelező érvényű döntést hoz, a besorolásnál alacsonyabb szint alkalmazására pedig javaslatot tesz az érintett szervnek.

4. §

Jogorvoslatok

(1) A hatóság döntései ellen a Ket. 109. § (1) bekezdésének a) pontja értelmében bírósági felülvizsgálatnak van helye.

(2) A hatóság határozatai ellen a Ket. 112. §-a értelmében újrafelvételi kérelem nem nyújtható be.

(3) A hatóság határozatainak felügyeleti jogkörben való visszavonására, módosítására a Ket. 114. § (4) bekezdése értelmében nincs lehetőség.

5. §

Az érintett szerv egyes kötelezettségei

(1) Az érintett szerv az Ibtv. 26. §-ára tekintettel, az Ibtv. 12. §-ában foglaltak végrehajtása érdekében – amennyiben a biztonsági szabályzat, elkészítése, vagy a biztonságért felelős személy, szervezet kijelölése objektív akadályba ütközik, vagy az érintett szerv számára különös nehézséget okoz – az Ibtv-ben meghatározott 60, illetve 90 napon belül a Hatóságot tájékoztatja, a teljesítés határidejének megjelölésével.

(2) Az elektronikus információs rendszer biztonságáért felelős személy – ideértve információs biztonsági szolgáltatást nyújtó vállalkozás tagjait és alkalmazottjait is – az érintett szerv igényeihez igazodva és annak rendelkezése szerint feladatát elláthatja
a) részmunkaidőben, vagy
b) a vonatkozó szerződésben meghatározott időtartamban,
c) több érintett szervnél.

(3) Az Ibtv. 12. § a) pontja szerinti tájékoztatás magában foglalja a vonatkozó munka-, megbízási, vagy más szerződés hatóság részére való megküldését, amelyhez csatolni kell az adott személy végzettségét, képzettségét igazoló okirat, illetve a szakterületi gyakorlatot igazoló okirat vagy nyilatkozat másolatát.

(4) Az Ibtv. 11. § (3) bekezdésének alkalmazásában a szervezet vezetője nem mentesül azon jogszabályban meghatározott kötelezettségek alól, amelyek a szervezet felett az információ biztonság tekintetében gyakorolt irányítási és ellenőrzési jogkörébe tartoznak.

(5) Amennyiben a szervezet adatkezelési, vagy adatfeldolgozási tevékenységéhez, vagy az elektronikus információs rendszere üzemeltetéséhez az Ibtv. hatályba lépése előtt megkötött szerződés alapján közreműködőt vesz igénybe, a biztonsági követelmények teljesítéséről azt nyilatkoztatni, a nyilatkozatot a hatóságot részére másolatban megküldeni köteles.

(6) Az Ibtv. 11. § (4) bekezdése alapján az ágazati szabályzók rendelkezésre állása esetén ezeket szervezeti szinten alkalmazni kell. Amennyiben a szakmai irányítást ellátó miniszter az ágazat, vagy az általa felügyelt központosított rendszer, illetve szolgáltatás tekintetében általános informatikai biztonsági szabályozást ad ki, szervezeti szinten csak annyiban kell egyedi szabályokat létrehozni, amennyiben ezt az érintett szervre érvényes egyedi jellemzők megkövetelik. A szakmai irányítást ellátó miniszter az egyedi szabályokat az ágazati, szervezeti, funkcionális, vagy földrajzi jellegzetességekre való tekintettel alakítja ki.

(7) Az Ibtv. 13. § (3) bekezdése szerinti biztonsági eseményt a hatóság által meghatározott módon, a biztonsági eseményre vonatkozó összes információ megadásával, dokumentum csatolásával soron kívül be kell jelenteni a hatóságnak. A hatóság a bejelentést soron kívül megvizsgálja, és annak alapján – a kormányzati, illetve ágazati eseménykezelő központok, illetve a szakhatóság, vagy más hatóság szükség szerinti bevonásával – megteszi a megfelelő intézkedéseket.

(8) Nem kell bejelenteni a hatóság felé azokat a biztonsági eseményeket, amelyeket az érintett szerv saját hatáskörében, biztonsági rendszerének üzemszerű működésével el tudott hárítani, és amelyek jelentős kárt, vagy működésbeli kiesést nem okoztak.

(9) Az érintett szerv a (7) és (8) bekezdések szerinti eseményekről nyilvántartást köteles vezetni, amely tartalmazza az esemény kapcsán tett intézkedéseket, és azok eredményét is.

(10) Amennyiben az érintett szerv megállapítja, hogy a biztonsági besorolás tekintetében a rendszereire, vagy reá irányadó követelményeket nem éri el, erről a hatóságot a cselekvési terv egyidejű megküldésével köteles tájékoztatni.

(11) Amennyiben az érintett szerv a reá irányadó biztonsági besorolás helyett alacsonyabb szintet állapít meg, annak okát részletes indoklással kell ellátnia.

6. §

A szakhatósági eljárás általános szabályai

(1) A Nemzeti Biztonsági Felügyelet (a továbbiakban: szakhatóság) az Ibtv 14. § (1) bekezdésében meghatározott hatóság szakhatóságaként az Ibtv. hatálya alá tartozó szervezetek elektronikus információs rendszereinek, rendszerelemeinek sérülékenység-vizsgálatát, valamint a biztonsági események adatainak műszaki vizsgálatát a jelen rendeletben meghatározottak szerint, a hatóság megkeresése vagy felkérése esetén, szakhatósági eljárás keretében vizsgálja.

(2) A sérülékenység-vizsgálati szakhatósági eljárás célja az esetleges biztonsági események bekövetkeztét megelőzően a szervezet elektronikus információs rendszere gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása az elektronikus információs rendszerek védelmének és biztonságának megerősítése érdekében.

(3) A sérülékenység-vizsgálati szakhatósági eljárás tárgya az adatok, információk kezelésére használt technikai (tipikusan elektronikus) eszközöknek, eljárásoknak, és kapcsolódó folyamatoknak, valamint az ezeket kezelő személyek együttesének az e rendeletben meghatározott célok érdekében és eljárásoknak megfelelően történő ellenőrzése.

(4) A biztonsági események műszaki vizsgálatára vonatkozó szakhatósági eljárás célja, hogy a bekövetkezett biztonsági események kivizsgálása révén
a) feltárja a biztonsági esemény bekövetkeztének okait, körülményeit,
b) behatárolja a biztonsági esemény által érintett elektronikus információs rendszerek körét,
c) javaslatot tegyen a biztonsági esemény által okozott kár elhárítására, és
d) a bekövetkezett biztonsági eseményből levonható tanulságokról tájékoztassa a biztonsági eseménnyel érintett szervezeteket, a hatóságot és a Központot annak érdekében, hogy a jövőben biztonsági esemény bekövetkezése megelőzhető legyen.

7. §.

Egyes szakhatósági eljárások

I. A sérülékenység-vizsgálati szakhatósági eljárás

(1) A szakhatóság sérülékenység-vizsgálati szakhatósági eljárását – az Ibtv. 14. § (2) a)-b) pontjában meghatározott, az elektronikus információs rendszerek osztályba sorolásának és a szervezetek biztonsági szintjei megállapításának, valamint az ezekre vonatkozó, a jogszabályban meghatározott követelmények teljesülésének ellenőrzése érdekében –a szakhatóság is kezdeményezheti a hatóságnál.

(2) A sérülékenység-vizsgálati szakhatóság eljárás ügyintézési határideje a 6. § (1) bekezdésben meghatározott vizsgálatok szerint:
a) külső vizsgálat esetén 30 nap,
b) webes vizsgálat esetén 30 nap,
c) belső vizsgálat esetén 30 nap,
d) wifi vizsgálat esetén 30 nap,
e) 3G/GPRS vizsgálat esetén 30 nap,
f) az emberi tényezőkön alapuló sérülékenységek vizsgálata esetén 30 nap.

(3) A szakhatóság vezetője a szakhatósági eljárásra irányadó határidőt annak letelte előtt egy alkalommal legfeljebb harminc nappal meghosszabbíthatja, és erről a vizsgálattal érintett szervezetet és a hatóságot értesíti.

(4) A sérülékenység-vizsgálati szakhatósági eljárás lezárásakor a szakhatóság sérülékenység-vizsgálati szakhatósági állásfoglalást készít, melyet a hatóság részére haladéktalanul megküld.

(5) A szakhatóság a sérülékenység-vizsgálati szakhatósági eljárás megindításáról szóló értesítéssel egyidejűleg a mulasztás jogkövetkezményeire történő figyelmeztetés mellett hiánypótlás keretében felhívja a vizsgálattal érintett szervezetet az eljárás lefolytatásához szükséges, egyedileg meghatározott dokumentumok, technikai információk és eszközök átadására, a szükséges hozzáférések biztosítására.

(6) A vizsgálattal érintett szervezet köteles az (1) bekezdésben foglalt adatokat, dokumentumokat, eszközöket és egyéb információkat a szakhatóság rendelkezésére bocsátani a hiánypótlási felhívásban foglaltak szerint, az értesítés kézhezvételétől számított 15 napon belül.

(7) Ha az eljárás során a tényállás tisztázása azt szükségessé teszi, a szakhatóság a vizsgálattal érintett szervezetet nyilatkozattételre hívja fel. Ha a vizsgálattal érintett szervezet a szakhatóság felhívására nem nyilatkozik, a szakhatóság a rendelkezésre álló adatok alapján dönt, vagy a hatóságot értesíti, hogy a szakhatósági eljárás lefolytatása nem lehetséges.

(8) A sérülékenység-vizsgálati szakhatósági eljárás keretében a szakhatóság a (12) bekezdésben meghatározott módszertan szerint folytatja le a vizsgálatot.

(9) Az eljárás kezdetén a szakhatóság sérülékenység-vizsgálati szakhatósági eljárást megalapozó dokumentációban (a továbbiakban: szakhatósági dokumentáció) rögzíti a feladatokat, célokat, a szigorú technikai és személyi feltételeket, a módszertant, az egyeztetések rendszerét, a vizsgálat várható befejezésének dátumát.

(10) A szakhatósági dokumentációt a szakhatóság 5 napon belül megküldi a vizsgálattal érintett szervezet részére.

(11) A vizsgálattal érintett szervezet a szakhatósági dokumentáció tartalmára a kézhezvételtől számított 8 napon belül észrevételt tehet, amelynek elfogadásáról a szakhatóság mérlegelési jogkörében dönt.

(12) A sérülékenység-vizsgálati szakhatósági eljárás során a szakhatóság a szakhatósági dokumentációban meghatározottak szerint az alábbi vizsgálatokat végzi el:
a) külső vizsgálat,

b) webes vizsgálat,
c) belső vizsgálat,
d) wifi vizsgálat,
e) 3G/GPRS vizsgálat,
f) emberi tényezőkön alapuló vizsgálat.

(13) A vizsgálat az (1) bekezdés a-e) pontjaiban meghatározott irányultságok tekintetében három típusú jogosultsági fázist tartalmazhat:
a) regisztrált felhasználói jogosultság nélküli vizsgálat,
b) regisztrált felhasználói jogosultsággal rendelkező vizsgálat és
c) adminisztrátori jogosultsággal rendelkező vizsgálat.

(14) A sérülékenység-vizsgálati szakhatósági eljárás lezárásaként kiadott elektronikus információs rendszereket érintő biztonsági vizsgálati szakhatósági állásfoglalás rendelkező része – a Ket. 44. § (6) bekezdésében foglaltak mellett – tartalmazza:
a) a rövid, közép és hosszú távú intézkedésekre vonatkozó intézkedési tervet,
b) az a) pont szerinti intézkedések becsült idő és költségigényét,
c) a szakhatósági eljárás költségeit.

(15) A szakhatósági állásfoglalás indokolása – a Ket. 44. § (6) bekezdésében foglaltak mellett – tartalmazza:
a) a sérülékenység-vizsgálati szakhatósági eljárás módszertanának leírását,
b) a sérülékenység-vizsgálati szakhatósági eljárás eredményeként a szakhatóság által feltárt sérülékenységek részletes technikai információit,
c) a szakhatóság által javasolt megoldásokat.

(16) A szakhatóság a vizsgálatot követően elkészített szakhatósági állásfoglalását hivatalosan megküldi a vizsgálattal érintett szervezet és a hatóság részére.

II. A biztonsági események adatainak műszaki vizsgálatára vonatkozó szakhatósági eljárás

(17) A szakhatóság a biztonsági események adatainak műszaki vizsgálatára vonatkozó szakhatósági eljárását az Ibtv. 14. § (2) bekezdés e) és 18. § a) pont aa) és ab) alpontjaiban meghatározottak szerint a hatóság felkérésére végzi.

(18) A felkérés mellékleteként a hatóság átadja a rendelkezésre álló, a vizsgálat elvégzéséhez szükséges dokumentumokat, technikai információkat

(19) A szakhatóság a mulasztás jogkövetkezményeire történő figyelmeztetés mellett hiánypótlás keretében felhívja a vizsgálattal érintett szervezetet a biztonsági események adatainak műszaki vizsgálatára vonatkozó eljárás lefolytatásához szükséges, egyedileg meghatározott dokumentumok, technikai információk és eszközök átadására, a szükséges hozzáférések biztosítására.

(20) A vizsgálattal érintett szervezet köteles a (3) bekezdésben foglalt adatokat, dokumentumokat, eszközöket és egyéb információkat a szakhatóság rendelkezésére bocsátani a hiánypótlási felhívásban foglaltak szerint, az értesítés kézhezvételétől számított 15 napon belül.

(21) Ha az eljárás során a tényállás tisztázása azt szükségessé teszi, a szakhatóság a vizsgálattal érintett szervezetet nyilatkozattételre hívhatja fel. Ha a vizsgálattal érintett szervezet a szakhatóság felhívására nem nyilatkozik, a szakhatóság a rendelkezésre álló adatok alapján dönt, vagy a hatóságot értesíti, hogy a szakhatósági eljárás lefolytatása nem lehetséges.

(22) Amennyiben a szakhatóság az eljárás befejezése mellett dönt, a szakhatóság írásban tájékoztatja a hatóságot az eljárás sikertelenségéről, amelynek indokolásában a vizsgálattal érintett szervezet mulasztó magatartását köteles feltüntetni.

8.§

Az ellenőrzési terv

(1) Az éves ellenőrzési tervet a hatóság minden év november 30-áig állítja össze, a szakhatóság és a kormányzati, illetve ágazati eseménykezelő központok, illetve az európai és nemzeti létfontosságú rendszerelemek nyilvántartására és a nyilvántartás adatainak kezelésére kijelölt szerv véleményének kikérésével.

(2) A hatóság az ellenőrzési terv végrehajtását az aktuális évet követő év március 1-jéig értékeli, és arról jelentést tesz az ellenőrzési tervet jóváhagyó minisztereknek.

(3) A hatóság vezetője az ellenőrzési tervben foglaltaktól – a szakhatósággal, a kormányzati eseménykezelő központtal, illetve ha az ügy jellege azt megkívánja az európai és nemzeti létfontosságú rendszerelemek nyilvántartására és a nyilvántartás adatainak kezelésére kijelölt szervvel egyeztetve – eltérhet, amennyiben olyan soron kívüli ellenőrzést, illetve ellenőrzéseket, vagy eljárásokat kell lefolytatnia, amelyek a magyar kiberteret, a nemzeti elektronikus adatvagyont, az állam és polgárai számára kiemelten fontos információs rendszereket súlyosan veszélyeztető fenyegetés elhárítását szolgálják.

(4) A hatóság vezetője az ellenőrzési tervtől való eltérésre vonatkozó javaslatát, ha az az eljárás sikerét nem befolyásolja, az ellenőrzési tervet jóváhagyó miniszterekkel előzetesen jóváhagyatja, ellenkező esetben azt utólagosan, az ellenőrzési terv értékeléséről szóló jelentésben bemutatja.

9. §

Jogkövetkezmények

(1) A hatóság az információbiztonsági követelmények teljesülése érdekében – a jogkövetkezmények kilátásba helyezésével – határidő tűzése mellett írásban szólítja fel az érintett szerv vezetőjét az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, illetve a biztonsági követelménysértés megszüntetésére, jogszabályban meghatározott kötelezettség teljesítésére, illetve az elvárt intézkedés megtételére.

(2) A hatóság soron kívül jár el, amennyiben az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, illetve a megsértett biztonsági követelmény súlyos biztonsági esemény bekövetkeztével fenyeget.

(3) Amennyiben az információbiztonságot veszélyeztető hiányosság kiküszöbölésére, a

mulasztás, pótlására, illetve a megsértett biztonsági követelmény helyreállítására ismételt felszólítás ellenére sem került sor, és az érintett szerv az intézkedés elmaradását objektív okokra hivatkozva kimenteni nem tudja, a hatóság az Ibtv-ben meghatározott jogkövetkezményt alkalmazza.

(4) A bírság ötvenezer forinttól ötmillió forintig terjedhet, amelyet a hatóság határozatának jogerőre emelkedését követő nyolc napon belül kell befizetni a hatóság Magyar Államkincstárnál vezetett számlájára.

(5) A hatóság a jogkövetkezmények alkalmazása során az alábbi szempontokat veszi figyelembe
a) az információbiztonságot veszélyeztető hiányosság, mulasztás, illetve a megsértett biztonsági követelmény súlyát,
b) történt-e súlyos biztonsági esemény, vagy ilyen esemény bekövetkeztének veszélye,
c) a biztonsági esemény hatását, vagy lehetséges hatását az érintett szervre, vagy más szervezetekre,
d) az érintett szerv magatartását, hatósággal való együttműködését,
e) az esemény egyedi, vagy ismételt jellegét.

(6) A bírság tekintetében az érintett szerv – legfeljebb 12 hónapra – a hatóságtól részletfizetési kedvezményt kérhet.

(7) A hatóság az összes körülmény mérlegelésével dönthet az Ibtv. 16. § (2)-(3) bekezdése szerinti intézkedések elhalasztásáról. A hatóság bármely intézkedést azonnal bevezethet, vagy mellőzhet amennyiben az információbiztonságot veszélyeztető hiányosság, mulasztás, illetve a megsértett biztonsági követelmény súlyos biztonsági esemény bekövetkeztével fenyeget, vagy ez be is következik.

10. §

Az információbiztonsági felügyelő kirendelése

(1) Az információbiztonsági felügyelő (a továbbiakban: felügyelő) kirendelése olyan hatósági intézkedés, amely alapján a felügyelőként kirendelt személy az érintett szerv jogszabályban meghatározott információ biztonsági követelmények érvényesítése érdekében a jogszabályban meghatározott jogokkal és kötelezettségekkel bír.

(2) A felügyelő kirendelését a hatóság kezdeményezi a miniszternél. A felügyelő kirendelésére vonatkozó javaslat tartalmazza a kirendelés indokait, a korábbi, az érintett szerv kapcsolatos intézkedéseit, egyben javaslatot tesz a felügyelő személyére, a kirendelés időtartamára. A miniszter az Ibtv-ben meghatározott esetek fennállása esetén jogosult dönteni a felügyelő kirendeléséről.

(3) Felügyelőként az rendelhető ki, aki a kirendelést vállalja, és rendelkezik vezetői gyakorlattal, amelynek időtartamába beleszámítható minden olyan közigazgatáson kívüli vezetői gyakorlat is, amelyet a tisztviselő egyéb munkavégzése irányuló jogviszony alapján látott el.

(4) A felügyelő egyidejűleg több érintett szervhez is – amennyiben a kirendelés indokai ezt lehetővé teszik – kirendelhető.

(5) A miniszter a megbízólevél kiállításával a felügyelőt határozott időtartamra rendeli ki az adott szerv információ biztonsági tevékenységének felügyeletére. A kirendelés meghosszabbítását a hatóság vezetője kezdeményezheti a kirendelés idejének lejárta előtt, legfeljebb egy alkalommal, a folyamatban lévő intézkedések lezárásáig. A kirendelés időtartamának meghatározásakor figyelemmel kell lenni a kötelezettségszegés súlyára és a fenyegetés elhárításához szükséges védelmi intézkedésekre. A kirendelésről szóló megbízólevél megfelelően tartalmazza a 2. § (12) bekezdése szerinti elemeket, valamint a kirendelésről szóló javaslatban megfogalmazott indokokat.

(6) Felügyelőnek nem rendelhető ki az a személy, aki
a) az érintett szervezettel munkavégzésre irányuló jogviszonyban áll,
b) a kirendelést megelőző három évben az adott szervezettel munkavégzésre irányuló jogviszonyban állt,
c) a kirendelést megelőző három évben az adott szervezetnél rendszeres és tartós megbízási vagy vállalkozási jogviszonyban áll, vagy állt,
d) az adott szerv vezetőjének, gazdasági vezetőjének vagy alkalmazottjának hozzátartozója, e minőségének fennállása alatt,
e) az adott szervezet képviselője, e minőségének fennállása alatt, illetve annak megszűnésétől számított három évig,
f) az, akitől az adott helyzet tárgyilagos megítélése üzleti érdekeltségből vagy egyéb okból nem elvárható (elfogultság),

(7) A felügyelő kirendelésének megszűnésére a megbízólevélben meghatározott időtartam letelte előtt akkor kerülhet sor, ha
a) ha a kirendelés oka elhárult és a felügyelő összefoglaló beszámolóját a hatóság elfogadta, vagy
b) a felügyelőt a miniszter visszahívja.

(8) A felügyelőt a miniszter akkor hívja vissza, ha
a) a hatóság megállapítja, hogy az adott szervnél a felügyelőnek felróhatóan nem érvényesülnek a biztonsági követelmények, vagy
b) az (5) bekezdésben írt, kizárásra okot adó körülmény merül fel, vagy a fennálló, a kizárásra okot adó körülmény a miniszter tudomására jut.

(9) A miniszter jogosult a (7) bekezdés b) pontja, illetve a (8) bekezdés esetén új felügyelő kirendeléséről gondoskodni. Az új felügyelő kirendelésére a 6. § (2) bekezdése alapján szintén a hatóság vezetője tesz javaslatot.
A felügyelő kirendelésének megszűnéséről a hatóság vezetője írásban tájékoztatja az érintett szerv vezetőjét.

(10) A felügyelő jogosult a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok betartásával, teljesítésével összefüggésben
a) az adott szerv vezetőitől és bármely dolgozójától írásbeli és szóbeli tájékoztatást, adatszolgáltatást kérni,
b) az érintett szerv információ technológiával kapcsolatos valamennyi dokumentumába, okiratába betekinteni, arról másolatot, kivonatot készíttetni,
c) az érintett szerv valamennyi helyiségébe belépni,
d) azonnali intézkedést javasolni a szerv vezetőjének a közvetlen fenyegetés elhárításához (működés korlátozása, leállítása),

e) intézkedést javasolni a jogszabályszerű működés kialakításához vagy helyreállításához, ennek keretében különösen szabályzatok felülvizsgálata,
f) kezdeményezni az elektronikus információs rendszereknek, vagy rendszerelemeknek a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény szerinti létfontosságú rendszerelemmé jelölését,
g) amennyiben olyan tény, adat, információ jut a felügyelő tudomására, amely akár büntető, szabálysértési, kártérítési, vagy fegyelmi eljárás kezdeményezését teszi indokolttá, jogosult eljárást kezdeményezni,
h) előzetesen véleményezni a működéssel kapcsolatos informatikai biztonságot is érintő intézkedéseket,
i) kifogással élhet az érintett szervezet által az Ibtv. alapján megtett vagy elmulasztott intézkedései, döntései tekintetében.

(11) A felügyelő köteles az érintett szervnél megbízólevelét bemutatni, továbbá
a) figyelemmel kísérni megbízatásának időpontjától kezdve az adott szervnél a jogszabályokban foglalt biztonsági követelmények és eljárások megvalósulását, a jogszabályokban előírt feladatok ellátását,
b) feltárni azokat az okokat, amelyek a nem teljesítéshez vagy esetleg a fenyegetés kialakulásához vezettek,
c) a b) pontban foglaltak és az érintett szerv működésének ismert feltételei alapján a szükséges intézkedések végrehajtására irányuló intézkedési tervet készíteni a szervezet részére,
d) azonnali intézkedéseket kezdeményezni, úgy hogy azok bevezetése nem lehetetleníti el az alaptevékenység ellátását, valamint azokról haladéktalanul értesíti a hatóságot,
e) betartani a titoktartási kötelezettségre vonatkozó szabályokat,
f) a felügyelő a megtett intézkedésekről a hatóságnak folyamatosan beszámol – a beszámolóban számot kell adni a megtett intézkedésekről, a biztonsági követelmények teljesüléséről, fejlődéséhez szükséges további szükséges intézkedésekről,
g) a felügyelő megbízatásának megszűnésekor összefoglaló beszámoló köteles készíteni a működéséről, ideértve a megtett intézkedéseket és azok eredményét, és a javasolt további intézkedéseket, amely elfogadásáról a hatóság dönt.

11.§

Kapcsolattartás az elektronikus információ biztonság szervezetrendszerével

(1) Az elektronikus információ biztonsági szabályok érvényesülésének biztosítására az Ibtv-ben megnevezett szervek tájékoztatási kötelezettsége körében:
a) az európai és nemzeti létfontosságú rendszerelemek nyilvántartására és a nyilvántartás adatainak kezelésére kijelölt szerv és a hatóság, valamint a szakhatóság, illetve a kormányzati eseménykezelő központ kölcsönösen tájékoztatják egymást az Ibtv. személyi hatálya alá tartozó szervek, illetve a létfontosságú rendszerelemek kapcsán feltárt, az információbiztonságot érintő megállapításaikról. A tájékoztatást soron kívül el kell végezni, amennyiben annak tárgya az információbiztonságot fenyegető veszélyforrást tár fel, vagy biztonsági eseményre utal. Az értesítés alapján az érintett szervek a hatáskörükbe tartozó intézkedést – egymással koordinálva – soron kívül megkezdik,
b) a kormányzati eseménykezelő központ tájékoztatja a hatóságot az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetéről, amellyel kapcsolatban a hatóság 5 napon belül az alakszerűség mellőzésével állást foglal. Az állásfoglalás elmaradása esetén a tervezetet elfogadottnak kell tekinteni

(2) A hatóság a Nemzeti Kiberbiztonsági Koordinációs Tanács részére éves jelentést készít, amely tartalmazza
a) az elvégzett ellenőrzések eredményét,
b) az Ibtv. alanyi és tárgyi hatálya tekintetében Magyarország kibertér biztonsági helyzetének értékelését,
c) a jelentéssel érintett időszak kiemelt eseményeit.

(3) A hatóság vezetője a Nemzeti Kiberbiztonsági Koordinációs Tanácsot eseti jelentésben tájékoztatja, ha olyan jelenséget, vagy folyamatokat észlel, amelyek Magyarország kiberbiztonsági helyzetére jelentős kihatással vannak.

(4) A hatóság az elektronikus információbiztonság növelése és az azonnali reagálás érdekében kormányzati információtechnológiai és hálózatbiztonsági információ-megosztási, incidens-kezelési együttműködési operatív fórumot működtethet. A fórum célja, az Ibtv. hatálya alá tartózó, a fórum tagjait delegáló szervek és szervezetek biztonsági szintjének emelése, az azonnali információ megosztás, az egyes sérülékenységek, fenyegetések és incidensek korai felismerése és egységes, gyors, kormányzati szintű kezelése, a veszély, fenyegetés mielőbbi elhárítása, illetve az erre való felkészülés. A fórum működését a tagok többsége által elfogadott Alapító Okirat, valamint szervezeti és működési szabályzat szabályozza.

Infokommunikációs ágazati hálózatbiztonsági központ

(5) A miniszter a hatóság útján felügyeli az infokommunikációs ágazati hálózatbiztonsági központot (a továbbiakban: IHK).

(6) Az IHK
a) működési szabályzatát a hatóság vezetője ellenjegyzi,
b) tevékenységéről a hatóság számára havi, negyedéves, illetve éves beszámolót készít,
c) vezetőjének kinevezésével és felmentésével, az IHK működésének lényegi kérdéseivel kapcsolatban a miniszter egyetértési jogot gyakorol.

(7) Az IHK feladatai:
a) a Nemzeti Távközlési Gerinchálózat végpontjainak védelme – ideértve az ezen működő rendszereket és rendszerelemeket is –, az ezekkel kapcsolatos preventív (megelőző) információ-megosztás és közvetlen biztonsági eseménykezelés,
b) együttműködés a kormányzati eseménykezelő központtal,
c) a kormányzati eseménykezelő központ, illetve más ágazati eseménykezelő központok tájékoztatása a tudomására jutott információbiztonságot érintő eseményekről, sérülékenységekről és fenyegetésekről,
d) a bejelentett biztonsági események fogadása, valamint az azok kezeléséhez szükséges operatív intézkedések megtétele és koordinálása,
e) a hatókörébe tartozó hálózatok tekintetében a hálózatbiztonság folyamatos helyzetértékelése, különös tekintettel a hálózat működése során keletkezett hálózat forgalmi adatok elemzésére,
f) folyamatosan elérhető 24 órás ügyelet fenntartása,
g) a biztonsági események kivizsgálása során a biztonsági események adatainak műszaki szempontú elemzése,

h) a biztonsági események adatainak gyűjtése, ezekről, valamint a hálózat forgalmi adatok elemzéséről – a hatókörébe tartozó hálózatok tekintetében – havonta jelentés készítése a hatóság részére,
i) együttműködés a hatósággal és a kormányzati eseménykezelő központtal,
j) a Tanúsítási Szervezettel kapcsolatos feladatok ellátása,
k) felkérésre szakmai közreműködés az egyes szervezetekkel az Ibtv. 11. § (1) bekezdés d), e) és f) pontjai szerinti tevékenységekben,
l) felkérésre informatikai biztonsági oktatóanyagok kidolgozása, illetve biztonsági oktatások tartása és szervezése az egyes szervezetek munkatársai számára,
m) szakmai közreműködőként a hatóság támogatása az Ibtv. 16. § (1) bekezdés e) pontja szerinti hazai információbiztonsági, és kibervédelmi gyakorlatok szervezésében,
n) szakmai közreműködőként a hatóság támogatása az Ibtv. 16. § (1) bekezdés f) pontja szerinti nemzetközi információbiztonsági és kibervédelmi gyakorlatok szervezésében és ezekben Magyarország képviselete,
o) a Nemzeti Távközlési Gerinchálózat végponti felhasználói tekintetében tudatosítási tevékenység ellátása a magyar társadalom információbiztonsági tudatossága növelése érdekében.

(8) Az IHK a hazai és nemzetközi hálózatbiztonsági feladatok megvalósítása érdekében a nemzeti hálózatbiztonság céljából fejlesztett alkalmazásokat működteti, illetve a folyamatban levő fejlesztéseket megvalósítja.

(9) Az IHK alapszolgáltatásokat nyújt, úgymint
a) információ-megosztás, ami a sérülékenységekről, fenyegetettségekről, káros szoftverekről és incidensekről napi, heti és rendkívüli -– kockázatértékeléssel ellátott – jelentések formájában történő általános illetve direkt tájékoztatás,
b) incidens-kezelési támogatás, ami a bekövetkezett incidenssel kapcsolatos bejelentések 0-24 órás kezelése és nyomon követése, koordináció az érintett hazai és nemzetközi szervezetek felé az incidenst kiváltó okok megszüntetésére illetve kezelésére, tanácsadás incidens analízis és kárenyhítés céljából egyes gazdálkodó szervezetek számára. Az IHK szolgáltatásai – kivéve a többségi állami tulajdonú gazdálkodó szervezeteket – nem zárják ki más ágazati eseménykezelő központ, vagy központok létrehozását, működtetését.

(10) Az IHK a (9) bekezdésben foglaltakon túl – külön szerződés szerint harmadik fél számára – értéknövelt szolgáltatást is nyújthat.

12.§

A Nemzeti Tanúsítási Rendszer

(1) Az Ibtv. 4.§-ában foglaltak megvalósítása érdekében a miniszter létrehozza és működteti az informatikai termékek megfelelőségének tanúsítására a Common Criteria for Information Technology Security Evaluation (a továbbiakban: CC) nemzetközi információ technológiai biztonsági értékelési szabványrendszer speciális információtechnológiai követelményeinek megfelelő Nemzeti Tanúsítási Rendszert, amelynek alapját képező nemzeti tanúsítási séma tekintetében a hatóság feladatai
a) az adminisztrációs teendők ellátása,
b) a CC rendszer kapcsán hazai és nemzetközi képviselet,
c) a tanúsítást végző Tanúsító Szervezet által végzett tevékenység felügyelete, az éves jelentés elfogadása, ellenőrzése,

d) a CC szabványrendszer szerinti nyilvántartás vezetése a tanúsított termékekről.

(2) A hatóságot a feladatai ellátásában tanácsadó fórum támogatja, amely a nemzeti tanúsítási sémával kapcsolatos stratégiai döntésekben véleményt fogalmaz meg, és ajánlásokat tesz. A tanácsadó fórum tagjai
a) a Tanúsító Szervezet vezetője,
b) a hatóság vezetője,
c) a kormányzati eseménykezelő központ felügyeletét ellátó minisztérium képviselője,
d) további állandó, vagy eseti meghívottak.

(3) A Tanúsító Szervezet feladata:
a) a termék és rendszer tanúsítások lefolytatása,
b) nyilvántartás vezetése a tanúsításokról,
c) az elvégzett tanúsítások utánkövetése és minőségbiztosítása,
d) nemzetközi képviselet a magyar tanúsítási sémához kapcsolódóan.

(4) A Vizsgáló Szervezetek végzik a termék és elektronikus információs rendszerértékeléseket a magyar tanúsítási séma alapján.

(5) Az elektronikus információs rendszerre vonatkozó elvárások jogszabályban meghatározott módon megkülönböztetik a szervezetre vonatkozó fizikai és adminisztratív, valamint a szervezeten belül az egyes elektronikus információs rendszerekre vonatkozó logikai védelmi intézkedéseket.

(6) A Tanúsító Szervezet a tanúsítási eljárása során a fizikai és adminisztratív követelmények teljesítését elfogadja, ha annak megfelelőségét az információbiztonsági irányítási rendszer megfelelőségének vizsgálatára akkreditált szervezet igazolja.

(7) Az elektronikus információs rendszer logikai követelményeknek való megfelelőség tanúsítása során a Tanúsító Szervezet megkövetelheti a biztonságilag kritikus, egyedi fejlesztésű termékeknek a 1. § (13) bekezdésében szereplő módszertanon alapuló biztonsági vizsgálatát, a vizsgálatra feljogosított nemzetközi, vagy hazai Vizsgáló Szervezet eredményét elfogadhatja.

(8) A logikai követelmények teljesítését termékek esetén a Tanúsító Szervezet kötelezően elfogadja, ha a vizsgálatot a CC szabványrendszer szerinti termékértékelésre jogosult magyar, vagy külföldi vizsgáló laboratórium végezte, és az megfelelő eredménnyel zárult. A Tanúsító Szervezet elfogadhatja a biztonságilag kritikus termékek esetében a hazai elfogadott Vizsgáló Szervezet értékelését is.

(9) Megfelelő eredménnyel zárult termékértékelések esetén is – illetve ha a Tanúsító Szervezet termékértékelési elvárást nem fogalmaz meg – a 4. és 5. biztonsági osztályba besorolt elektronikus információs rendszerek esetében az 1. § (13) bekezdésében szereplő tanúsítvánnyal kell igazolni, hogy a termékértékelés során felállított feltételrendszer elvárásai az adott rendszer vonatkozásában teljesülnek, valamint az adott elektronikus információs rendszerre teljesülnek a biztonsági osztályba sorolásának megfelelően az Ibtv. 5. § a) pontjában szereplő adatokra vonatkozó bizalmassági, sértetlenségi és rendelkezésre állási, valamint a b) pontjában szereplő zárt, teljes körű, folytonos és kockázatokkal arányos követelményei.

(10) Amennyiben jogszabály eltérően nem rendelkezik, közbeszerzési eljárás keretében csak olyan egyedi fejlesztésű információ technológiai termék szerezhető be, amely az 1. § (13) bekezdése szerinti tanúsítvánnyal rendelkezik.

13. §

Ez a rendelet 2013. július 1-jén lép hatályba.

14. §

Módosító rendelkezések

(1) Az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről szóló 212/2010. (VII. 1.) Korm. rendelet (a továbbiakban: Statútum) 92. § (1) bekezdés f) pontja a következő fd) alponttal egészül ki:
[szakmai irányítást gyakorol a közigazgatási intézmények, állami vagy részben állami tulajdonban lévő gazdasági társaságok, hírközlési, informatikai tevékenysége felett, ide értve a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatalát is, ennek keretében:]

„fd) a Nemzeti Informatikai Biztonsági Hatóság felügyeli az állami és önkormányzati, valamint a létfontosságú rendszereket és rendszerelemeket működtető szervek és szervezetek elektronikus információbiztonsági tevékenységét,”

(2) Statútum 92. § (1) bekezdése a következő n) és m) pontokkal egészül ki:
[A miniszter az informatikáért, a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért és az űrkutatásért való felelőssége körében:]

„n) felügyeli a Nemzeti Informatikai Biztonsági Hatóságot,
m) gyakorolja a Nemzeti Tanúsítási Rendszerrel kapcsolatos döntési jogkört, felügyeli és irányítja annak működését, képviseli Magyarországot a nemzetközi minőséghitelesítési eljárásában.”

15. §.

Átmeneti rendelkezések

A 3. § (1) bekezdés alkalmazásának tekintetében az Európai Unió más tagállamában végzett, jelen rendelet hatálybalépésekor már folyamatban levő adatkezelési tevékenységet a hatóság felé a 3. § (2) bekezdés szerinti adattartalommal soron kívül be kell jelenteni.