

TERVEZET

A Kormány

/2015. (. .) Korm. rendelete

a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről

A Kormány

a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 290. § (1) bekezdés c) pontjában,

az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 88. § a) pontjában,

a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 437. § c) pontjában, valamint

a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény 180. § (1) bekezdés a) pontjában

kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. §

E rendelet hatálya

a) a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény szerinti hitelintézetre és pénzügyi vállalkozásra,

b) az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény szerinti pénzforgalmi intézményre, elektronikuspénz-kibocsátó intézményre és a Posta Elszámoló Központot működtető intézmény pénzforgalmi szolgáltatási és elektronikus pénzkibocsátási tevékenységére,

c) a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény szerinti biztosítóra és viszontbiztosítóra, valamint

d) a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény szerinti befektetési vállalkozásra és árutőzsdei szolgáltatóra

(a továbbiakban együtt: intézmény) terjed ki.

2. §

(1) Az intézmény kialakítja a pénzügyi szolgáltatási, a kiegészítő pénzügyi szolgáltatási, biztosítási és viszontbiztosítási és az azzal közvetlenül összefüggő tevékenységének, a befektetési szolgáltatási tevékenységének és kiegészítő szolgáltatásának ellátásához használt informatikai rendszer biztonságával kapcsolatos szabályozási rendszerét, valamint gondoskodik az informatikai rendszer kockázatokkal arányos védelméről. A szabályozási rendszerben meg kell határozni az információ-technológiával szemben támasztott követelményeket, a használatából adódó biztonsági kockázatok felmérésére és kezelésére vonatkozó szabályokat az informatikai vállalatirányítás, a tervezés, a fejlesztés és a beszerzés, valamint az üzemeltetés, a monitorozás és független ellenőrzés területén.

(2) Az intézmény az informatikai rendszer biztonsági kockázatelemzését szükség szerint, de legalább két évente felülvizsgálja és aktualizálja.

TERVEZET

(3) Az informatika alkalmazásából fakadó biztonsági kockázatok figyelembevételével az intézmény meghatározza a szervezeti és működési rendeket, a felelősségi, a nyilvántartási és a tájékoztatási szabályokat, a folyamatba épített ellenőrzési követelményeket és szabályokat.

3. §

(1) Az intézmény kiépíti az informatikai rendszere biztonságos működtetését felügyelő informatikai ellenőrző rendszert és azt folyamatosan működteti.

(2) A biztonsági kockázatelemzés eredményének értékelése alapján a biztonsági kockázattal arányos módon gondoskodni kell legalább az alábbiakról:

a) a rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról,

b) az informatikai biztonsági rendszer önvédelmét, kritikus elemei védelmének zártságát és teljeskörűségét biztosító ellenőrzésekről, eljárásokról,

c) a rendszer szabályozott, ellenőrizhető és rendszeresen ellenőrzött felhasználói adminisztrációjáról (hozzáférési szintek, egyedi jogosultságok, engedélyezésük, felelősségi körök, hozzáférés naplózás, rendkívüli események),

d) olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza, alkalmas a naplózás rendszeres (esetleg önműködő) és érdemi értékelésére, valamint lehetőséget nyújt a nem rendszeres események kezelésére is,

e) a távadatátvitel bizalmasságáról, sértetlenségéről és hitelességéről,

f) az adathordozók szabályozott és biztonságos kezeléséről, valamint

g) a rendszer biztonsági kockázattal arányos vírus- és más rosszindulatú program elleni védelméről.

(3) Az intézmény tevékenysége ellátásához, nyilvántartásai naprakész és biztonságos vezetéséhez a biztonsági kockázatelemzés alapján indokolt védelmi intézkedéseket megvalósítja, és rendelkezik

a) informatikai rendszerének működtetésére vonatkozó utasításokkal és előírásokkal, valamint a fejlesztésre vonatkozó tervekkel,

b) minden olyan dokumentációval, amely az üzleti tevékenységet közvetlenül vagy közvetve támogató informatikai rendszerek folyamatos és biztonságos működését - még a szállító, valamint a rendszerfejlesztő tevékenységének megszűnése után is - biztosítja,

c) a szolgáltatások ellátásához szükséges informatikai rendszerrel, valamint a szolgáltatások folytonosságát biztosító tartalék berendezésekkel, illetve e berendezések hiányában az ezeket helyettesítő egyéb - a tevékenységek, illetve szolgáltatások folytonosságát biztosító - megoldásokkal,

d) olyan informatikai rendszerrel, amely lehetővé teszi az alkalmazási környezet biztonságos elkülönítését a fejlesztési és a tesztelési környezettől, valamint a megfelelő változáskövetés és változáskezelés fenntartását,

e) az informatikai rendszer szoftver elemeiről (alkalmazások, adatok, operációs rendszer és környezetük) olyan helyreállítási tervekkel, biztonsági mentésekkel és mentési renddel (mentések típusa, módja, visszatöltési és helyreállítási tesztek, eljárási rend), amelyek az adott rendszer helyreállíthatóságát a rendszer által nyújtott szolgáltatás kritikus helyreállítási idején belül lehetővé teszik,

f) jogszabályban meghatározott nyilvántartás ismételt előhívására alkalmas adattároló rendszerrel, amely biztosítja, hogy az archivált anyagokat a jogszabályokban meghatározott ideig, de legalább öt évig, bármikor visszakereshetően, helyreállíthatóan megőrizték, valamint

g) a szolgáltatásai folyamatosságát akadályozó rendkívüli események kezelésére szolgáló tervvel.

TERVEZET

(4) A (3) bekezdés *e)* pontja szerinti mentéseket kockázati szempontból elkülönítetten és tűzbiztos módon kell tárolni, valamint gondoskodni kell a mentések forrásrendszerrel azonos szintű hozzáférési védelméről.

4. §

(1) Az intézménynél mindenkor rendelkezésre kell állnia

- a)* az általa fejlesztett, megrendelésére készített informatikai rendszer felépítésének és működtetésének az ellenőrzéséhez szükséges rendszerleírásoknak és modelleknek,
- b)* az általa fejlesztett, megrendelésére készített informatikai rendszernél az adatok szintaktikai szabályainak, az adatok tárolási szerkezetének,
- c)* az informatikai rendszer elemeinek az intézmény által meghatározott biztonsági osztályokba sorolási rendszerének,
- d)* az adatokhoz történő hozzáférési rend meghatározásának,
- e)* az adatgazda és a rendszergazda kijelölését tartalmazó dokumentumnak,
- f)* az alkalmazott szoftvereszközök jogtisztaságát bizonyító szerződéseknek, valamint
- g)* az informatikai rendszert alkotó ügyviteli, üzleti szoftvereszközök teljes körű és naprakész nyilvántartásának.

(2) A szoftvereknek együttesen alkalmasaknak kell lenniük

- a)* a működéshez szükséges és jogszabályban előírt adatok nyilvántartására,
- b)* a pénzeszközök és a pénzügyi eszközök biztonságos nyilvántartására,
- c)* az intézmény tevékenységével összefüggő országos informatikai rendszerekhez történő közvetlen vagy közvetett csatlakozásra, ideértve a pénzforgalmi számlák cégbíróság felé történő bejelentését is,
- d)* a tárolt adatok ellenőrzéséhez való felhasználására, valamint
- e)* a biztonsági kockázattal arányos logikai védelemre és a sérthetlenség védelmére.

5. §

Az intézmény a belső szabályzatában meghatározza az egyes munkakörök betöltéséhez szükséges informatikai ismeretet.

6. §

Ez a rendelet 2016. január 1-jén lép hatályba.

7. §

Hatályát veszti a pénzügyi intézmények, a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 535/2013. (XII. 30.) Korm. rendelet.