Irányelv informatikai háttér biztosítása szolgáltatás nyújtásához

Tartalomjegyzék

1. Irányelv célja és keretei

A jelen irányelv célja, hogy orientálja a szolgáltatókat az informatikai háttérszolgáltatások vonatkozásában tett ajánlásokkal, ugyanakkor egyúttal meghagyja számukra a technikai megoldás megválasztásánál – beleértve a kapcsolódási felületekre tett javaslatok kidolgozását is – a megfelelő mozgásteret, hogy a szolgáltatás kialakítása ne jelentsen aránytalanul nagy terhet számukra.

A Közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) 2011. évi módosítása jelentősen módosította az elektronikus ügyintézésre vonatkozó szabályokat, lehetővé téve és előírva az elektronikus megoldások minél szélesebb körű alkalmazását.

1.1. Irányelv koncepciója

Az informatika gyors fejlődésére és sokszínűségére tekintettel olyan szabályozási környezetet célszerű kialakítani, ahol az egyes megoldások részletszabályai már csak a legszükségesebb mértékben, mintegy minimumkövetelményként kerülnek jogszabályban meghatározásra, így lehetőség van az ügyintézés kiszolgálásában közreműködő számára az innovatív megoldások folyamatos követésére és rendszerszintű alkalmazására, a technológia fejlődéséből adódó lehetőségek folyamatos kihasználására.

Az egységesség, együttműködő képesség – mind a hazai rendszerek egymás közötti, mind az EU vonatkozó rendszereivel való jelenkori és esetleges jövőbeli integrációjának – megtartása és lehetővé tétele érdekében ugyanakkor a szabályozási modell útmutató jellegű ajánlások kibocsájtását rendelte el, amelyek a hatályos jogszabályok figyelembevételével lefektetik a szolgáltatásnyújtás műszaki feltételeit és körülményeit.

Az informatikai alkalmazások jelentős száma egyre növekvő hardver és szoftver beruházásokat, infrastrukturális fejlesztéseket, kvalifikált üzemeltetési személyzetet igényel, ezért költséghatékonysági és a rugalmas bővíthetőségi szempontból sok területen terjed az informatikai háttér szolgáltatásának, mint kiemelt és külön szakterületet lefedő tevékenységnek az igénybe vétele. Ez alapján indokolt, hogy a felügyelet külön SZEÜSZ alapján irányelvet fektessen le a különböző funkcionalitásokat nyújtó, de részben vagy teljesen hasonló informatikai hátteret igénylő szolgáltatások megvalósítására.

Ez az irányelv a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló kormányrendelet (a továbbiakban: SZEÜSZR.) 14. §-a alapján, a SZEÜSZ-ök egységes nyújtása és igénybevétele, az együttműködési képesség biztosítása érdekében kerül meghatározásra.

Tekintettel arra, hogy jelen dokumentum best-practice alapon megfogalmazott szakmai ajánlást tartalmaz az érintett SZEÜSZ tárgykörében, de nem specifikál alacsony szintű

implementációs szempontokat, a szerzőt a gyakorlati megvalósítások következményeivel kapcsolatban csak korlátozott felelősség terheli.

1.2. Jogszabályi háttér

Az irányelv egyúttal elősegíti az alábbi jogszabályok egységes alkalmazását is:

- *2004. évi CXL. Törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (a továbbiakban: Ket.),*
- *83/2012. (IV. 21.) Korm. Rendelet a szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról (SZEÜSZR),*
- *84/2012. (IV. 21.) Korm. Rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről (84/2012),*
- *85/2012. (IV. 21.) Korm. Rendelet az elektronikus ügyintézés részletes szabályairól (85/2012)*

Az elektronikus ügyintézés részletes szabályairól szóló 85/2012. (IV. 21.) Korm. rendelet 3. § (1) bekezdése a következőket írja elő:

> *3. § (1) Az elektronikus kapcsolattartás lehetőségét biztosító hatóság az elektronikus kapcsolattartás és elektronikus ügyintézés lehetőségét az elektronikus ügyintézési felügyelet (a továbbiakban: felügyelet) által kiadott ajánlásban meghatározott műszaki követelményeknek megfelelő informatikai rendszer útján biztosítja.*

Ez a Ket.-ben előírt új ügyintézési modell értelmezéséhez, gyakorlati alkalmazásához szükséges ajánlások kibocsájtását teszi a felügyelet feladatává.

A szabályozott elektronikus ügyintézési szolgáltatásokról és az állam által kötelezően nyújtandó szolgáltatásokról szóló SZEÜSZR. 14.§ (1) bekezdése a következőket írja elő:

> *14. § (1) A felügyelet a SZEÜSZ-ök egységes nyújtása és igénybevétele, az együttműködési képesség biztosítása érdekében ajánlásokat bocsát ki. A felügyeletnek tehát a szabályozott elektronikus ügyintézési szolgáltatások nyújtására, együttműködésük biztosítására is ajánlásokat kell kibocsájtania.*

Az elektronikus ügyintézés megvalósítása érdekében a Ket. a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól az alábbiak szerint értelmezi az elektronikus ügyintézéssel kapcsolatos szolgáltatást:

> *172. § E törvény alkalmazásában:*
>
> *d) elektronikus ügyintézéssel kapcsolatos szolgáltatás:*
>
> *da) a hatóság által az elektronikus ügyintézés megvalósítása érdekében kialakított*

informatikai háttér tekintet nélkül arra, hogy az informatikai háttér biztosítása során harmadik fél szolgáltatásait igénybe vette-e és milyen mértékben, vagy

db) a da) pontban meghatározott eseten kívül jogi személy, jogi személyiség nélküli szervezet által a hatóság vagy az ügyfél számára az elektronikus ügyintézés megvalósítása vagy használata érdekében ingyenesen vagy ellenérték fejében nyújtott, információs társadalommal összefüggő szolgáltatás

A SZEÜSZR. V. fejezete (AZ EGYES SZABÁLYOZOTT ELEKTRONIKUS ÜGYINTÉZÉSI SZOLGÁLTATÁSOK RÉSZLETES KÖVETELMÉNYEI) tartalmaz egy olyan, általános informatikai szolgáltatásra vonatkozó követelményt, mely a konkrét szabályozott elektronikus ügyintézési szolgáltatásoknak a szolgáltatásokhoz közvetlenül nem kapcsolódó, de azok nyújtásához szükséges informatikai háttér biztosítására vonatkozik az alábbi megfogalmazásban:

37. Informatikai háttér szolgáltatása

101. § (1) Az elektronikus ügyintézés megvalósítása érdekében kialakított informatikai háttér szolgáltatása keretében a SZEÜSZ szolgáltató

a) az ügyfelek, hatóságok, illetve hatóságon belül az ügyintézésben érintett ügyintézők elérhetőségét biztosító elektronikus rendszert, hálózatot vagy annak egy részét üzemeltet, illetve

b) olyan gépi és szoftver eszközöket biztosít és üzemeltet, amelyek közvetlenül nem részesei az elektronikus ügyintézési szolgáltatásnak, de annak nyújtásának feltételét képezik.

(2) Az (1) bekezdés a) pontja szerinti szolgáltatás a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter által kiadott rendeletben meghatározott feltételek és műszaki előírások szerint nyújtható.

(3) A hatóság az (1) bekezdés b) pontja alá tartozó eszközök, rendszerek üzemeltetése során a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter által kiadott rendeletben meghatározott műszaki, technikai és biztonsági előírások szerint jár el.

(4) Amennyiben technikai sajátosság, vagy nyilvánvaló gazdaságossági szempont mást nem indokol, az informatikai háttér szolgáltatása kapcsán szükséges hálózati feltételeket a Nemzeti Távközlési Gerinchálózat igénybevételével kell megteremteni.

A fentiek alapján hálózati szolgáltatás kivételével (melyre indokolt esetek kivételével csak az NTG vehető igénybe) elérhetőséget biztosító elektronikus rendszert, vagy hardver és szoftver eszközök biztosítására vonatkozó ajánlást nyújt az informatikai háttér szolgáltatása SZEÜSZ. Amennyiben a háttérszolgáltatás valamely eleme nem Magyarország területén működik,

vonatkozik rá az alább idézett kiemelés is a 2013. évi L. törvényből, amely az állami és önkormányzati szervek elektronikus információbiztonságáról az informatikai rendszerekre és az azokban tárolt adatokra fogalmaz meg általános és információbiztonsági követelményeket:

2. A törvény hatálya

2. § (1) E törvény rendelkezéseit kell alkalmazni:
a) a központi államigazgatási szervekre, a Kormány és a kormánybizottságok kivételével,
b) a Köztársasági Elnöki Hivatalra,
c) az Országgyűlés Hivatalára,
d) az Alkotmánybíróság Hivatalára,
e) az Országos Bírósági Hivatalra és a bíróságokra,
f) az ügyészségekre,
g) az Alapvető Jogok Biztosának Hivatalára,
h) az Állami Számvevőszékre,
i) a Magyar Nemzeti Bankra,
j) a fővárosi és megyei kormányhivatalokra,
k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulásokra,
l) a Magyar Honvédségre.

(2) E törvény rendelkezéseit kell alkalmazni:
a) az (1) bekezdésben meghatározott szervek és ezen szervek számára adatkezelést végzők,
b) a jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói,
c) az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek védelmére.

3. § (1) A 2. § (1) bekezdés a)–k) pontjában megjelölt szervek által kezelt adatok és a 2. § (2) bekezdés b) pontjában megjelölt szervezetek által kezelt, a nemzeti adatvagyon részét képező adatok Magyarország területén üzemeltetett elektronikus információs rendszerekben, valamint diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetőek.

(2) A 2. § (2) bekezdés c) pontjában megjelölt elektronikus információs rendszerek – az (1) bekezdésben meghatározott kivétellel – az Európai Unió tagállamai területén üzemeltethetőek.

(3) A 2. § (1) bekezdés a)–k) pontjában megjelölt szervek által kezelt adatok elektronikus információs rendszerei az elektronikus információs rendszerek biztonságának felügyeletét ellátó szervezeti egység (a továbbiakban: hatóság) engedélyével vagy nemzetközi szerződés alapján az Európai Unió tagállamainak területén belül üzemeltetett elektronikus információs rendszerekben is kezelhetőek.

(4) A törvény hatálya alá tartozó elektronikus információs rendszert működtető, nem Magyarországon bejegyzett vállalkozásnak Magyarország területén működő képviselőt kell kijelölnie, aki az e törvényben foglaltak végrehajtásáért a szervezet vezetőjére vonatkozó szabályok szerint felel.

1.3. Alkalmazói kör

Jelen irányelv az informatikai háttér szolgáltatást biztosító szabályozott elektronikus ügyintézési szolgáltatóknak kíván segítséget nyújtani.

Az informatikai háttér szolgáltatása SZEÜSZ lehetséges szolgáltatói:

- *hatóság,*
- *hatóságnak nem minősülő olyan személy, aki a szabályozott elektronikus ügyintézési szolgáltatást ügyfelek vagy hatóságok számára ingyenesen vagy ellenérték fejében elérhetővé teszi,*
- *egyéb SZEÜSZ-t megvalósító szolgáltató, amely a szolgáltatáshoz közvetlenül nem kapcsolódó, de annak nyújtásához szükséges informatikai hátteret a saját maga által nyújtott szolgáltatáshoz maga biztosítja.*

Az informatikai háttér szolgáltatása SZEÜSZ lehetséges igénybevevői:

(1) alkalmazói szoftver szolgáltatása esetén:

- *Közigazgatási hatóságok, amelyek alkalmazottaik számára elterjedt szoftveralkalmazásokhoz (például irodai programokhoz vagy e-mail szoftverhez) hozzáférést kívánnak biztosítani;*
- *Közigazgatási hatóságok ügyfelei (végfelhasználók), akik közvetlenül használnak szoftveralkalmazásokat, akár saját maguk, akár egy szervezet nevében;*
- *szoftveralkalmazások adminisztrátorai, akik alkalmazásokat konfigurálnak a hatóságok vagy azok ügyfelei számára.*

(2) platform szolgáltatás esetén:

- *elektronikus ügyintézési alkalmazások fejlesztői, akik alkalmazói szoftvereket terveznek és implementálnak;*
- *elektronikus ügyintézési alkalmazások tesztelői, akik megfelelő tesztkörnyezetekben futtatják az alkalmazásokat;*
- *elektronikus ügyintézési alkalmazások közzétevői, telepítői;*

- *elektronikus ügyintézési alkalmazások adminisztrátorai;*
- *közvetve az elektronikus ügyintézési alkalmazások felhasználói (hatóságok hatóságok ügyintézői, hatóságok ügyfelei), számukra közvetlenül alkalmazói szoftver szolgáltatásként jelenik meg az ügyintézési alkalmazás.*

(3) hardver alapinfrastruktúra szolgáltatása esetén:

- *elektronikus ügyintézési alkalmazások fejlesztői,*
- *elektronikus ügyintézési alkalmazások alaprendszerének rendszeradminisztrátorai, operátorai.*

Az informatikai háttér szolgáltatása SZEÜSZ a fenti logikai felosztás kombinációjaként is nyújtható, továbbá a SZEÜSZ más szabályozott elektronikus ügyintézési szolgáltatások háttérszolgáltatásaként történő megvalósítása esetében a háttérszolgáltatást nyújtó szervezet egyben a szolgáltatás igénybevevője is lehet.

2. Irányelv funkcionális alapjai

Lényeges célkitűzés a SZEÜSZ-ök szolgáltatásait megvalósító rendszerek skálázhatósága a teljesítményigények jövőbeli várható növekedésének biztonságos kiszolgálása érdekében, valamint azok minél szélesebb körű rugalmassága. Cél, hogy a szolgáltatás felhasználói részéről jelentkező igények változása, ill. szélesedése esetén a rendszereken elvégzendő módosítások mind költség-, mind időhatékonyság szempontjából kezelhető mértékűek legyenek.

Az elektronikus ügyintézési szolgáltatásokat, de általában az elektronikus szolgáltatásokat az ügyfelet közvetlenül érintő felületen kívül több alapul szolgáló informatikai réteg alkotja. Az állampolgárok, a hatóságok ügyintézői a konkrét SZEÜSZ-funkciókkal lépnek interakcióba, de ezek működéséhez szükség van egy informatikai háttérbázisra, megbízhatóan működő és biztonságos, fizikai és logikai rétegekbe sorolható erőforrásokra, ahogyan azt a fentebb idézett kormányrendelet szövege is kimondja: elektronikus rendszerre, gépi és szoftveres eszközökre. (Ezeket kiegészítik a fizikai és logikai erőforrások és intézkedések működési rendjét kontrolláló adminisztratív eljárások.) A fizikai rétegbe tartoznak a hálózati, kommunikációs alapinfrastruktúra, a központosított vagy fizikailag több helyre szétosztott adatközpontok, létesítmények az ott lévő hardverekkel. Logikailag a hardveren különböző technológiával kialakított futtatási környezetekben működő operációs rendszerek, informatikai keretrendszerek, a fizikai és felhasználói programok közötti köztes rétegek működnek, a végfelhasználónál pedig maguk a SZEÜSZ-alkalmazások üzemelnek, és ez utóbbiakkal találkozik közvetlenül az állampolgár és a hatóság ügyintézője.

Jelen irányelv az informatikai háttér szolgáltatásában a közvetlen hálózati infrastruktúrán kívüli erőforrásokra, háttérszolgáltatásokra vonatkozik. A fizikai hálózati infrastuktúra szolgáltatón kívüli részeit különösen indokolt esetek kivételével a Nemzeti Távközlési Gerinchálózat adja, a belső hálózat és az annak üzemeltetéséhez szükséges alacsony szintű szoftveres környezet részletes tárgyalása ugyanakkor nem képezi jelen irányelv célját: egyrészt a szolgáltatást nyújtó számára ez szükségtelenül szigorú és specifikált feltételeket írna elő, másrészt pedig az informatikai iparág gyors fejlődése következtében a feltételek szakszerűsége és időtállósága már rövid távon sem biztosítható.

A szabályozott elektronikus ügyintézési szolgáltatás informatikai hátterét az illetékes hatóság (közigazgatási hatóság, államigazgatási szerv, önkormányzat) kialakíthatja, üzemeltetheti

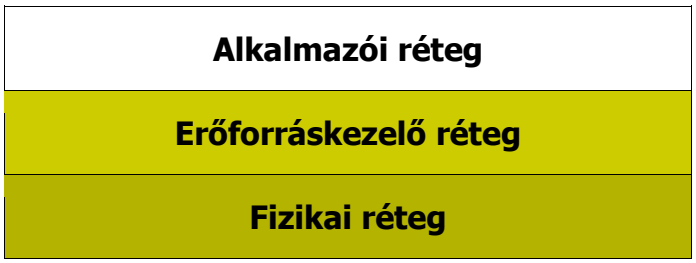
a) *saját maga (például saját gépterem, saját hardverek, vásárolt programok saját szakembergárdával való üzemeltetése);*

b) *teljesen vagy részlegesen kiszervezheti IT-szolgáltatással foglalkozó állami vagy piaci szereplőnek, azaz a közigazgatási megrendelő a tevékenysége informatikai hátterét adó elemek egészének vagy részének üzemeltetésére mást bíz meg, amennyiben az a Nemzeti Távközlési Gerinchálózat használatára vonatkozó előírásnak megfelel;*

c) *felhő alapú informatikai megoldással, amikor a közigazgatási megrendelő a felhő alapú*

informatika lehetőségei közül választ.

A jogszabályokból levezethető, hogy az informatikai háttér szolgáltatása SZEÜSZ két kulcsfontosságú eleme az elektronikus ügyintézési szolgáltatásokhoz informatikai erőforrások nyújtása mind a rendszerek, mind az adatok biztonságának fenntartásával. Az informatikai háttér szolgáltatása összetett szolgáltatás, és emiatt, valamint a megvalósíthatóság többféle szempontja miatt rendszerezést igényel. A rendszerezési szempontok rámutatnak, hogy ez a szolgáltatás több önállóan értelmezhető szolgáltatásként is nyújtható. Mivel az „informatikai háttér szolgáltatása" fogalom általános érvényű, ugyanakkor széleskörű alkalmazása a gyakorlatot tekintve kikerülhetetlen, ezért jelen irányelv a feltételek alacsonyabb absztrakciós szintű előírásának mellőzésével, de nemzetközileg elismert és előremutató technológiák elvi alkalmazása szintjén fogalmazza meg a követelményeket. Az informatikai háttér szolgáltatása az alábbi ábrán látható három fő réteg egy vagy több rétegében valósulhat meg.



Háromrétegű szolgáltatási modell

Az informatikai háttér szolgáltatásakor e három rétegbe eső összetevők (hardver és szoftver elemek) nyújtását kell megvalósítania a SZEÜSZ szolgáltatónak. Abból a tényből, hogy az informatikai háttér szolgáltatását külön SZEÜSZ szolgáltatásként nevezi meg a jogalkotó, következik, hogy nem feltétlenül az elektronikus ügyintézésben részt vevők (hatóságok) biztosítják közvetlenül az elektronikus ügyintézési szolgáltatás informatikai hátterét, hanem önálló SZEÜSZ szolgáltató végezheti ezt a szolgáltatást részlegesen vagy teljesen. Ez a szolgáltatásnyújtás az érintett felek (szolgáltatást nyújtók és szolgáltatást igénybe vevők) között történhet hagyományos informatikai központok kialakításával, de történhet új, az Európai Unió által kormányzati megoldásként is perspektivikusnak ítélt felhő alapú rendszerek használatával is. Jelen dokumentum mindkét architektúra kialakítására vonatkozóan állapít meg szempontokat.

3. Felhőalapú szolgáltatási infrastruktúra

A felhő technológia (cloud) igénybevételére már számos állam törekszik, sorra jelennek meg az esettanulmányok a cloud sikeres alkalmazásáról az Egyesült Államokban, Nagy-Britanniában, Németországban, Japánban, más angolszász országokban, illetve többek között Kínában is. A felhő technológia állami, illetve hatósági szervek körében történő terjedése mellett az alkalmazhatóság példájaként szolgálnak továbbá az olyan, az informatikai szakterületen ismert kereskedelmi cégek is, amelyek kiterjedtségük és felhasználóik nagy számának következtében egyedülállóan nagy adatmennyiségeket kezelnek, tárolnak és mozgatnak, igen magas (>99,9%) szolgáltatási rendelkezésre állási mutató mellett (Google, Facebook, stb).

Az állami célkitűzések mellett, azokkal párhuzamosan, a cloud technológia elterjesztésére, intenzív felhasználására törekszik az Európai Unió is. A felhő alapú szolgáltatások egyértelmű kultúraváltást jelentenek a felhasználói magatartásban, mert bármilyen informatikai szolgáltatás (hardver, szoftver egyaránt) immár nem beruházás révén, hanem a szolgáltatásra irányuló igény szerint, ún. on-demand módon juthat el a felhasználóhoz, azaz a SZEÜSZ igénybevevőjéhez.

Egy felhő alapú informatikai rendszer olyan szolgáltatási keretrendszer, amely lehetővé teszi, hogy a szolgáltatók által nyújtott elosztott számítástechnikai erőforrásokat (szervereket, tárolókat, hálózatokat, alkalmazásokat, stb.) igény alapján, gyorsan konfigurálható és kioszthető és visszaadható módon, kényelmesen el lehessen érni a kapcsolt hálózat bármely pontjáról, a lehető legkevesebb irányítási erőfeszítéssel vagy szolgáltatói közbeavatkozással. A szolgáltatás nem szükségszerű, de gyakori eleme a virtualizáció és elosztott számítástechnikai technológiák használata. A virtualizáció technikai előnye, hogy egy adott feladatra igényelt környezet könnyen és a későbbi változtathatóságot szem előtt tartva megteremthető, eközben pedig a meglévő infrastruktúra jelentős változtatás nélkül felhasználható. Az elosztott rendszerek technikai előnye, hogy a kialakított infrastruktúra a terheléshez jól alkalmazkodik (skálázható), valamint adott esetben redundanciát is magában foglaló felépítése más rendszerekhez képest hibatűrőbbé teszi.

A felhő, belső működését tekintve, a hagyományos informatikai infrastruktúra ismert és a gyakorlatban is széleskörben használt elemeiből építkezik, ugyanakkor egy absztrakt keretrendszert is nyújt a szolgáltatónál belső infrastruktúrával megvalósított, vagy kiszervezett (azaz külső féltől bérelt, igénybe vett) erőforrásokhoz, és ebben a keretben az informatikai szolgáltatások nyújtása három kategóriába sorolható:

- *alkalmazói szoftver*
- *hardver és fejlesztési környezet a befogadó (hoszt) szoftverplatformmal*
- *hardver alapinfrastruktúra*

Felhő esetén adatfeldolgozást a felhőszolgáltató maga nem végez, csak biztosítja az

erőforrásokat a megrendelő számára az adatfeldolgozáshoz.

A hagyományos IT-erőforrások kiszervezését alapvetően a profiltisztítás és az azzal járó gazdasági előnyök vezérlik, esetenként a speciális szakértelem biztosítása indokolja. A felhő alapú megoldások ezen felül az erőforrások jobb kihasználását, energiahatékonyságot, skálázhatóságot, valamint igényalapú felhasználást biztosítanak. A felhő alapú informatikai rendszerek az elektronikus ügyintézésben – és általában az államigazgatásban – résztvevők számára az alábbi előnyöket kínálják:

- ***Megbízhatóság és rendelkezésre állás:*** *a cloud computing szolgáltatások mögött jellemzően folyamatosan jelentős fejlesztések és beruházások vannak annak érdekében, hogy a szolgáltatást megfelelő minőségben tudják nyújtani. A legtöbb felhőszolgáltatás földrajzilag különböző pontokon elhelyezett, komoly méretű adatközpontokkal történik, amelyek nagy rendelkezésre állást biztosítanak. Mindez a felhőszolgáltató informatikai biztonsági és adattárszolgáltatási ismeretei, valamint az incidenskezelés hatékonyabbá tétele révén a biztonsági szempontok érvényesülése terén is előnyökkel jár.*

- ***Helyfüggetlenség:*** *egy felhőalapú szolgáltatás jellemző előnye, hogy a szolgáltatás a kapcsolt hálózatról tipikusan bárhonnan könnyen elérhető. A szolgáltatás maga is lehet független egy adott szerverközponttól. A felhő technológia így az erőforrások széles körű hálózati hozzáférésére épít az erőforrások és képességek biztosításában, ami az állampolgárok számára megnyíló elektronikus ügyintézés alapfeltétele.*

- ***Erőforrások hatékony kezelése:*** *a felhőalapú szolgáltatások egyrészt segítenek felszabadítani az alattuk lévő informatikai infrastruktúrák hardvereire rakódó terheket, és lehetővé tenni, hogy az erőforrásokat más, olyan célokra lehessen átcsoportosítani, ahová az adott időszakban fokozottabb igény jelentkezik. Másrészt jelentős mennyiségű emberi erőforrást takarítanak meg, hiszen számos tevékenység elvégzését a felhőszolgáltató maga vállalja. Ezzel az erőforrások igény szerinti kezelése és használata, a hardverhibák és csúcsidőszakok teljesítménycsökkenésének jó kezelhetősége jellemzi a technológiát.*

- ***Skálázhatóság:*** *gazdaságossági szempontok érvényesülése a felhő technológia szoftveres támogatása által, a hardver elemek kihasználásának hatékony jellegéből adódóan; az elektronikus ügyintézési igényekkel kapcsolatos informatikai igények változásának hatékonyabb követhetősége.*

- ***Költséghatékonyság:*** *felhőalapú technológia alkalmazásakor a szolgáltató a számítástechnikai erőforrásokat összevonja, így azokkal egyszerre több ügyfelet is ki tud szolgálni (feltéve, hogy az igénybe vevő szervezet adatvédelmi és biztonsági követelményei ezt lehetővé teszik). A fizikai és virtuális erőforrásokat (tárakat, CPU, memória, hálózati sávszélesség) dinamikusan, az igények szerint kiosztja, felszabadítja és újraosztja.*

A közigazgatásban résztvevő megrendelők számára mérlegelendő szempont lehet, hogy az informatikai háttérszolgáltatás költségei dinamikusan, a használat függvényében alakuljanak. Ilyen esetben szintén előnyös lehet a felhőszolgáltatás igénybevétele, szemben a hagyományos informatikai infrastruktúra esetén inkább jellemző, erőforráskihasználástól független, statikus költségvonzatú megoldással.

A felhő keretrendszer két kulcsfontosságú megközelítési módja a telepítési és a szolgáltatási modell. A telepítési modell azt határozza meg, hogy ki nyújtja a felhőszolgáltatásokat, a szolgáltatási modell pedig azt határolja be, hogy milyen kategóriájú informatikai háttérszolgáltatások állnak a szolgáltatás igénybevevőinek rendelkezésére.

Jelen irányelv a felhőalapú rendszerek tekintetében három telepítési modellt vesz tekintetbe: a nyilvános felhőt, a közösségi felhőt és a magánfelhőt. A negyedik típusban, a hibrid felhőben rejlő lehetőségek a felhő alapú informatikai megoldások magyarországi tapasztalatai hiányában jelen irányelvben nem szerepelnek. A három telepítési alapmodell kulcseleme, hogy a felhőinfrastruktúra kiknek (mely közigazgatási szervezetek számára) ajánl informatikai szolgáltatásokat.

- ***Magánfelhő**: Az informatikai infrastruktúrát kizárólag egy szervezet használja (a szervezet számára dedikált kommunikációs kapcsolaton keresztül, vagy saját infrastruktúrán megvalósított felhővel).*
- ***Közösségi felhő**: Az informatikai infrastruktúrát kizárólag olyan szervezetek felhasználóinak adott közössége használja, akikre közös érdekeik alapján azonos szabályok vonatkoznak (például: célkitűzés, biztonsági követelmények, jogszabályi megfelelési szempontok).*
- ***Nyilvános felhő**: Az informatikai infrastruktúra és számítási erőforrások használata a nagyközönség számára nyitott (az Interneten keresztül).*

A telepítési modell mellett a felhő alapú informatikai rendszerek másik kulcskérdése a szolgáltatási modell, melynek három alaptípusa az informatikai háttér szolgáltatása fentebb megnevezett három rétegéhez illeszkedő módon: a szoftver mint szolgáltatás (SaaS[1]), platform mint szolgáltatás (PaaS[2]) és (hardver)infrastruktúra mint szolgáltatás (IaaS[3]). A szolgáltatási modellek funkcionálisan absztrakciós szintjükben térnek el egymástól.

Szoftver mint szolgáltatás (SaaS): a szolgáltató a szolgáltatás igénybevevői számára lehetőséget biztosít a felhő alapú infrastruktúrán futó szolgáltatói alkalmazások használatára. Az alkalmazások különböző klienseszközökről érhetők el, akár vékony kliens interfészen (például web-böngészőn), akár program interfészen keresztül.

[1] SaaS: Software as a Service

[2] PaaS: Platform as a Service

[3] IaaS: Infrastructure as a Service

Platform mint szolgáltatás (PaaS): a szolgáltató a szolgáltatás igénybevevői számára lehetőséget biztosít a felhasználó által létrehozott vagy vásárolt alkalmazásoknak a felhő alapú infrastruktúrára való telepítésére, a szolgáltató által támogatott programozási nyelvek, könyvtárak, szolgáltatások és eszközök használatával. A fejlesztői környezetet a felhőszolgáltató általában a saját platformjának megfelelően, egyedileg alakítja ki.

Infrastruktúra mint szolgáltatás (IaaS): a szolgáltató a szolgáltatás igénybevevői számára lehetőséget biztosít a feldolgozó, tároló, hálózati és egyéb alapvető számítástechnikai erőforrások használatára. Az ügyfél így képes tetszőleges szoftvert telepíteni és futtatni, beleértve operációs rendszereket és alkalmazásokat is.

A felhő alapú informatika erősségei mellett nem elhanyagolhatók az ismert és – a technológia összetett és változó jellegéből adódóan – még megismerés alatt álló gyengeségei és veszélyei sem. Az előnyökre is igaz az, hogy nem minden telepítési/szolgáltatási modellt jellemzik egyforma mértékben a felhő lényegi jellemzői (van olyan kombináció, amely nem sokban különbözik a hagyományos saját adatközponttól, mint például helyszíni magánfelhő kis és közepes szervezeteknél). A SZEÜSZ szolgáltatókra vonatkozó irányelvek tekintetében az adatvédelmi és információbiztonsági szempontok elsődlegessége miatt a veszélyek figyelembe vétele is fontos szempont, emiatt a biztonsággal kapcsolatos követelmények is hangsúlyosak a SZEÜSZ erőforrásnyújtási képességei mellett. A lehetséges gyengeségek és veszélyek elsősorban két fő forrásból származhatnak:

- *az informatikai tevékenységek fölötti irányítás és felügyelet hiányából;*
- *a jogszabályoknak való meg nem felelésből.*

Jogi szempontból és az adatok feletti felügyelet oldaláról nézve a nyilvános felhők jelentik a nagyobb kockázatot a közösségi és magánfelhőkhöz képest, melynek okai:

- *felhőtulajdonosok (nyilvánosfelhő-szolgáltatók) és a szolgáltatás igénybevevői (közigazgatás szereplői) ütköző érdekei;*
- *nyilvános felhők tulajdonosa lehet nem magyar személy vagy szervezet is, így adott esetben nagyok vagy akár pontosan felmérhetetlenek lehetnek az ezzel járó gazdasági, politikai vagy nemzetbiztonsági kockázatok is;*
- *a biztonság és az erőforrás-kiosztás rugalmasságának átláthatóságát biztosító vállalásaik, a biztonsági incidensek kezelési szintje (jelentések, riasztások, utólagos, ún. forensic analízis, stb.) az üzleti modellből adódóan általában alacsonyabb szinten vannak a másik két telepítési modellhez és a hagyományos IT-szolgáltatásoknál alkalmazott szinthez képest;*
- *bárki igénybe veheti őket.*

A nyilvános felhők országok közötti átjárhatósága jogszabályi akadálya a nyilvános felhők alkalmazhatóságának, mert a 2013. évi L. törvény 3. § (1) pontja értelmében az elektronikus ügyintézésben tárolt, továbbított, kezelt adatok „*Magyarország területén üzemeltetett*

elektronikus információs rendszerekben, valamint diplomáciai információs célokra használt zárt célú elektronikus információs rendszerben kezelhetőek".

Az informatikai tevékenységek fölötti irányítás és felügyelet szemszögéből nézve, a fent említett három telepítési modell közül az információbiztonsági szempontból érzékeny alkalmazások és adatok tekintetében a magánfelhő, valamint indokolt esetben a közösségi felhő SZEÜSZ szolgáltatásként való megvalósítása fogadható el, a nyilvános felhő használata az elektronikus közszolgáltatások körében jelenleg nem engedélyezhető.

A magánfelhő esetén a felhő alapú infrastruktúrát kizárólag egy szervezet (jelen esetben az érintett hatóság és annak ügyfelei) használja, amely több igénybevevőből (például közigazgatási szervezet részlegei) állhat. A felhő lehet a hatóság tulajdona, menedzselheti, üzemeltetheti a szervezet, de menedzselheti és lehet tulajdonos és üzemeltető egy harmadik fél is (SZEÜSZ szolgáltató). Ezek kombinációja is elképzelhető, és a felhő létesítése és üzemeltetése történhet helyszíni adatközpontban vagy attól távoli helyen. A magánfelhő biztosítja az igénybevevő részére a legnagyobb szabadságot a testreszabásra és felügyeletre, különösen, ha helyszíni magánfelhő-telepítésről van szó, amikor a felhasználó szervezet saját infrastruktúráján épül ki az informatikai háttérszolgáltatás és ő is menedzseli azt.

A magánfelhő kialakítására többféle kezdeményezés lehetséges. Kialakítható teljesen új adatközpontként; meglévő adatközpont egy része vagy egésze átalakítható magánfelhővé; lehetséges a kevert erőforrás-kihasználási megoldás, amikor meglévő számítógépeken alakítják ki a felhőt, felhőhasználati és felhőhasználaton kívüli időre bontva az erőforrások hozzárendelését.

A nyilvános és magánfelhő közötti sávba eső közösségi felhő esetén a felhasználói célcsoport jelenti a jellemző különbséget a magánfelhőhöz képest. A felhőinfrastruktúrát kizárólag olyan közigazgatási egységek adott közössége (azok ügyintézői és ügyfelei) használja, amelyek valamilyen közös közigazgatási szempont alapján szerveződnek erre (például: egymásra épülő ügyintézési lánc különböző hatóságok között, hasonló vagy megegyező biztonsági követelményekkel; hasonló vonatkozó szabályzók, megfelelési szempontok által vezérelt tevékenységek). A közösségen belül egy vagy több szervezet lehet a tulajdonos, ugyanakkor a kezelő és az üzemeltető lehet harmadik fél is. A felhő létesítése történhet a telephelyen vagy attól távol is.

3.1. Folyamatokhoz kapcsolódó szolgáltatási funkciók

Az informatikai háttér szolgáltatása SZEÜSZ két fő funkciója az elektronikus ügyintézési szolgáltatásokhoz informatikai erőforrások nyújtása és a rendszerek és adatok biztonságának fenntartása.

Az informatikai erőforrások nyújtása felhőalapú architektúra esetén a három alaprétegbe eső erőforrások szerint történhet:

- *alkalmazói szoftver nyújtása;*

- *platform infrastruktúra nyújtása;*
- *hardver alapinfrastruktúra nyújtása.*

A felhő terminológiában ezeknek megfelel a SaaS, PaaS és IaaS modell szerinti szolgáltatás. A korábban megnevezett okok alapján a három szolgáltatást kétféle kiépítésben biztosíthatja a SZEÜSZ szolgáltató: magánfelhőben és közösségi felhőben. Ugyanakkor a szolgáltatási modellek is vetnek fel kérdéseket az informatikai tevékenységek fölötti irányítás és felügyelet tekintetében, ezért a SZEÜSZ szolgáltatókra a kiépítés (magán, közösségi) mellett a szolgáltatási modellek (SaaS, PaaS, IaaS) szempontjai szintén követelményeket írnak elő.

A szolgáltatási modell nem csak a szolgáltatási kategóriát határozza meg, hanem azt is, hogy a felhőarchitektúra két fő szereplője – a szolgáltatás igénybe vevője és a szolgáltatás nyújtója – között milyen hatásköri és felelősségi határok húzódnak.

A SZEÜSZ szolgáltató a szolgáltatásokat külön-külön is nyújthatja, de biztosíthatja ezek kombinációját is. Jelen irányelv az alábbiakban mindhárom szintet áttekinti.

3.1.1. Alkalmazói szoftver szolgáltatása (SaaS)

A SaaS a SZEÜSZ használóját a felhő alapú infrastruktúrán futó szolgáltatói alkalmazások használatára jogosítja fel. Az alkalmazások különböző klienseszközökről érhetők el, akár vékony kliens interfészen, akár program interfészen keresztül. A felhőhasználó nem menedzseli és nem felügyeli az alapul szolgáló felhőinfrastruktúrát, ideértve a hálózatot, szervereket, operációs rendszereket, tárolókat vagy az egyedi alkalmazások lehetőségeit. Ez alól néhány, korlátozott számú, felhasználó-specifikus alkalmazási beállítás kivétel lehet. A biztonsági szolgáltatásokat is nagyrészt a felhőszolgáltató valósítja meg.

A SZEÜSZ szolgáltató az alábbi SaaS kategóriájú szolgáltatásokat biztosítja:

- *felhő infrastruktúrán szoftveralkalmazások közzététele, konfigurálása, karbantartása, frissítése az elvárt szolgáltatási szinten;*
- *az alkalmazások, a biztonság és a felhőinfrastruktúra menedzselése;*
- *adott alkalmazások igény szerinti használatához való hozzáférés nyújtása, beleértve a felhasználók azonosítását és a jogosultságok ellenőrzését*
- *alkalmazói adatok kezelése (például mentések és – amennyiben az adatok bizalmassági szintje lehetővé teszi és a megbízók felhatalmazást adtak a szolgáltatónak – adatmegosztás ügyfelek között).*

Az alkalmazás és az infrastruktúra menedzselésével és felügyeletével kapcsolatos felelősségek nagy részét a SaaS szolgáltató viseli (kivéve néhány esetleges alkalmazás adminisztrálását, mely az ügyfél hatáskörébe tartozhat).

A SaaS szolgáltatáshoz a SZEÜSZ szolgáltató biztosíthatja

- *saját maga a SaaS szerinti szolgáltatások működéséhez szükséges erőforrásokat (PaaS, IaaS);*
- *vagy igénybe vehet más, az alkalmazáshoz szükséges és megfelelő informatikai háttérszolgáltatást (infrastruktúra- és platformszolgáltatást).*

A SZEÜSZ felhőszolgáltató teljes mértékben felelős az IT hardver alapinfrastruktúra- és a köztes szoftverinfrastruktúra-rétegek üzemeltetéséért, valamint adminisztrátori felügyeletet gyakorol a szolgáltatott alkalmazói szoftver fölött. A szolgáltatást igénybe vevő szervezet a SaaS alkalmazás által rendelkezésre bocsátott alkalmazásspecifikus erőforrások fölött gyakorol felügyeletet, és csak korlátozott, alkalmazásfüggő adminisztratív befolyással bír az alkalmazás tekintetében.

A szolgáltató felelős az alkalmazás telepítéséért, konfigurálásáért, frissítéséért, menedzseléséért; feladatai közé tartozik a felhasználói szabályzatok érvényre juttatása, számlázás, problémakezelés.

A hagyományos informatikai megoldásokhoz és szoftverközzétételhez képest a SaaS-felhők esetén az alkalmazásszintű logika nagy része a szolgáltató szerverein hajtódik végre, amihez az ügyfelek által használt kliensprogramok, leggyakrabban webböngészők folyamatos, megbízható és biztonságos működése szükséges.

3.1.2. Platform infrastruktúra szolgáltatása (PaaS)

Ez a típus a SZEÜSZ igénybevevője számára biztosított szolgáltatás az igénybevevő által létrehozott vagy vásárolt alkalmazásoknak a felhőinfrastruktúrára való telepítése, a szolgáltató által támogatott programozási nyelvi környezetek, kiszolgáló függvénykönyvtárak, szolgáltatások és eszközök használatával. A fejlesztői környezetet a felhőszolgáltató a saját platformjának megfelelően, egyedileg is kialakíthatja. Az ügyfél nem menedzseli és nem vezérli az alapul szolgáló felhőinfrastruktúrát, ideértve a hálózatot, szervereket, operációs rendszereket vagy tárakat, de ellenőrzése van a telepített alkalmazások fölött, és lehetőség szerint az alkalmazást befogadó (hosztoló) környezet konfigurációs beállításai fölött. A biztonsági szolgáltatások megvalósításának feladata megoszlik a felhőszolgáltató és felhőhasználó között.

A SZEÜSZ szolgáltató az alábbi PaaS kategóriájú szolgáltatásokat biztosítja:

- *a platformhoz megfelelő informatikai infrastruktúra menedzselése*
- *felhőszoftverek üzemeltetése, amelyek a platformhoz biztosítják a komponenseket (futási szoftverkörnyezet, adatbázisok, middleware elemek);*
- *az informatikai eszközök és futtató erőforrások használata az alkalmazások*

fejlesztéséhez, teszteléséhez, közzétételéhez és adminisztrálásához.

A PaaS szolgáltatáshoz a SZEÜSZ szolgáltató biztosíthatja

- *saját maga a PaaS szerinti szolgáltatások működéséhez szükséges erőforrásokat (IaaS);*
- *vagy igénybe vehet más, megfelelő infrastruktúra szolgáltatást.*

A SZEÜSZ felhőszolgáltató teljes mértékben felelős az IT hardver alapinfrastruktúra és a köztes szoftverinfrastruktúra operációs rendszereinek, azok komponenseinek, a hálózati eszközöknek a működéséért és felügyeletéért. A köztes infrastruktúra-rétegben biztosítja az ügyfélalkalmazások futtatási, fejlesztői környezetét, ezek fölött adminisztratív felügyeletet gyakorol, ő alakítja ki a programozási modellt, az ügyfélalkalmazások aktivizálódásának feltételeit, követi az ügyféltevékenységet menedzsment- és monitorozási okokból. Az alkalmazói programokkal kapcsolatban nincs felelőssége ebben a szolgáltatási modellben, magukért a PaaS infrastruktúrára megvalósított alkalmazói programokért a szolgáltatást igénybe vevő hatóság vagy szervezet felelős.

A PaaS felhők esetén is az SaaS modellhez hasonlóan igaz, hogy az alkalmazásszintű logika nagyobb része hajtódik végre a szolgáltató erőforrásain, mint a hagyományos IT-megoldások esetén, és a PaaS nyújtása jelentős terhet ró a felhőhasználó ügyfél böngészőjére (vagy a vékony kliensekre) abban a tekintetben, hogy megbízható és biztonságos kapcsolatnak kell kiépülnie a szolgáltató rendszere felé, továbbá a különböző PaaS-alkalmazások és -fiókok között az elkülönítés megvalósuljon.

3.1.3. Hardver alapinfrastruktúra szolgáltatása (IaaS)

A SZEÜSZ igénybevevője számára biztosított lehetőség a feldolgozó, tároló, hálózati és egyéb alapvető számítástechnikai erőforrás használatra bocsátása. A felhasználó így képes tetszőleges szoftvert telepíteni és futtatni, beleértve operációs rendszereket és alkalmazásokat is. Az ügyfél nem menedzseli és nem felügyeli az alapul szolgáló felhőinfrastruktúrát, de ellenőrzést gyakorol az operációs rendszer, a tárak és a telepített alkalmazások fölött, és adott esetben korlátozott befolyással bír a hálózati komponensek kiválasztására (például hoszt-tűzfalak). Az alapinfrastruktúrán túlmutató biztonsági szolgáltatások biztosítása elsősorban a felhőhasználó (hatóság vagy annak ügyfele) hatáskörébe tartozik.

A SZEÜSZ szolgáltató az alábbi IaaS kategóriájú szolgáltatásokat biztosítja:

- *biztonságos és ellenőrzött hozzáférés virtuális számítógépekhez, hálózaton elérhető tárakhoz és hálózati infrastruktúra-elemekhez (például tűzfalakhoz, konfigurációs eszközökhöz);*

- *A szolgáltatást biztosító infrastruktúra-elemek karbantartása, műszaki felügyelete, fizikai sérülésmentességének és a biztonsági szolgáltatás fizikai aspektusainak (például klimatizált és őrzött gépterem vagy géptermek, szünetmentes tápellátás, stb.) garantálása.*

Az IaaS kategóriájú erőforrás-szolgáltatás esetén a köztes szoftverréteget további egymásra épülő részekre lehet osztani, melyekkel kapcsolatos SZEÜSZ-hatáskör is különbözik. A napjainkban egyre gyakoribb virtualizációs megoldásokat alkalmazó esetben például az operációs rendszer által reprezentált réteg két alrétege: az alacsonyabb (privilegizáltabb) réteg a virtuálisgép-monitor (VMM), más néven hypervisor, azaz az ún. gazda (host) operációs rendszer, és e fölött az ún. vendég (guest) operációs rendszer. A felhő alapú IaaS-szolgáltatásnál rendszerint alkalmazott hypervisor hozza létre a hardveren az egy vagy több virtuális gépet (Virtual Machine, VM) az igénybevevő számára. Amikor egy ügyfél hozzáférést bérel egy géphez, a VM az ő számára egy adminisztrálható tényleges hardverként jelenik meg, amit a szolgáltatóhoz hálózaton küldött parancsok segítségével vezérel. Ennek az absztrakciónak az átláthatóságát az infrastruktúra szolgáltatója biztosítja. A virtuális gépen fut ugyanakkor a vendég operációs rendszer. Amennyiben a szolgáltató teljes virtualizációs technológiát használ, akkor az ügyfél számára nyitott az út bármilyen támogatott operációs rendszerszoftver betöltéséhez.

A SZEÜSZ szolgáltató teljes körű felügyeletet gyakorol a fizikai hardver fölött, és adminisztratív kontrollt a hardvervezérlési réteg (hypervisor) réteg fölött. Az ügyfél kéréssel élhet a felhő felé új virtuális gépek létrehozása és menedzselése céljából, de ennek teljesüléséhez szükséges, hogy a kérés megfeleljen a szolgáltató szolgáltatói szabályzatban rögzített erőforráskiosztási szabályainak. A hypervisoron keresztül a szolgáltató rendszerint hálózati funkciókhoz nyújt interfészeket, amelyeket az ügyfelek testre szabott virtuális hálózatok konfigurálására használhatnak a szolgáltatói infrastruktúrán belül. A felhőhasználók általában teljes mértékben felügyelik a virtuális gépen számukra vagy általuk kialakított operációs rendszer működését, és az afölötti szoftverrétegeket.

Ez a felépítés jelentős felügyeleti feladatot ad az igénybevevői oldalnak a szoftveres infrastruktúra vonatkozásában, ezért az igénybevevő szervezetnek vállalnia kell a hagyományos számítástechnikai erőforrások működtetését, frissítését és konfigurálását a biztonság és megbízhatóság érdekében. Az IaaS szolgáltatásmodellje jelentősen eltér a SaaS- és PaaS-felhőktől, melyekben az előbb említett IaaS-szempontok az ügyfelek számára transzparens módon kezeltek.

3.2. Informatikai biztonsági és adatbiztonsági funkciók

Az IT-biztonság és adatvédelem a szolgáltatási rétegek minden szintjét és mindegyik telepítési modellt érinti, és a SZEÜSZ szolgáltatókkal szemben követelményeket támaszt. A konkrét elvárás függ a szolgáltatási és a telepítési modelltől, de mindkettőnél az adott lényegi elem (telepítés vagy szolgáltatás) fölötti irányítás és felügyelet elvesztése vagy megtartása, illetve ezek mértéke áll a fókuszban. A felhő infrastruktúra nem sok új veszélyt hoz magával (bár a

lényegi jellemzőkből adódóan ilyenek is akadhatnak, például az egyes adattulajdonos szervezetek be tudják-e pontosan azonosítani a rendszerük tárhelyeihez hozzáférő felhasználókat), inkább a hagyományos hálózati környezetben meglévő fenyegetések hangsúlyeltolódásáról és kezelési felelősségeivel kapcsolatos változásokról van szó.

Az adatok és az elektronikus információs rendszerek biztonságáért a feldolgozást végző és adattulajdonos szervezet (hatóság) a felelős, ezt szem előtt tartva kell a különböző rétegbeli szolgáltatások esetén a jelen irányelvben szereplő követelményeket a SZEÜSZ informatikai háttér szolgáltatójától elvárni.

Nem önmagában a telepítési modell az, ami elsődlegesen meghatározza a biztonsági és adatvédelmi elvárásokat. A követelményeket értelmezni lehet és kell a telepítéstől, sőt a felhő alapú technológiától függetlenül. A megvalósított modell kiegészíti ezeket néhány valóban a modelltől függő tényezővel. Minden esetben az informatikai háttér szolgáltatását nyújtó szolgáltató által biztosított garancia, a biztonsági és adatvédelmi intézkedések átláthatósága és erőssége azok a megfontolások, amelyek közigazgatási alkalmazások megfelelő szolgáltatójává tesznek egy SZEÜSZ szolgáltatót.

3.3. Telepítéstől független követelmények

Az alábbi követelmények az informatikai háttér szolgáltatásának általános követelményei (hagyományos adatközpont vagy felhő esetén is értelmezhetőek, utóbbi esetén a felhőjellemzők adott szempont szerinti nagyobb kihasználásának maximalizálása a cél).

A SZEÜSZ informatikai háttér szolgáltatójának

- *képesnek kell lennie a szolgáltatást igénybe vevő közigazgatási szervezet számára biztonságos és megbízható hálózati hozzáférést biztosítani (ezt biztosíthatja saját maga vagy igénybe vehet ezt a célt teljesítő, megfelelő szolgáltatást);*
- *képesnek kell lennie az ügyfél feldolgozási igényeit úgy kielégíteni, hogy a terhelés rendelkezésre álló erőforrások közötti szétosztása a szolgáltatást igénybe vevők számára ne okozzon fennakadást;*
- *a szolgáltatott erőforrások (szerverek, géptermek) menedzseléséhez a szakértői állományát folyamatosan képeznie kell;*
- *képesnek kell lennie a vonatkozó dokumentumokban meghatározott csúcsterhelési időszakok kezelésére, valós időben sok felhasználó kiszolgálására (nagy tömegű adatimportálás, exportálások, nagy teljesítményigényű és/vagy kritikus feldolgozási folyamatok kiszolgálása).*

3.4. Telepítés szerinti IT biztonsági és adatvédelmi követelmények

Az adatvédelmi és információbiztonsági követelményeket az informatikai háttérszolgáltatás többféle paramétere alapján lehet megfogalmazni. A követelmények egyik oldalról függnek a felhőszolgáltatás telepítési modelljétől, a nyújtott szolgáltatástól. A másik oldalról pedig az IT biztonság elvárásait és az ezekkel kapcsolatos felelősségi (szerepköri, hatásköri) kérdéseket kell számba venni. Ez a fejezet ezen szempontrendszer alapján közelít a követelmények megfogalmazásakor.

3.4.1. Magánfelhő

A magánfelhő lehet a szervezet tulajdona, menedzselheti, üzemeltetheti a szervezet, de menedzselheti és lehet tulajdonos és üzemeltető egy harmadik fél is. Ezek kombinációja is elképzelhető, és a felhő létesítése (hosztolása) történhet a telephelyi adatközpontban vagy attól távoli helyszínen. Kiszervezett esetben a felelősségi határok az adott szolgáltatásmodelltől függenek.

A helyszíni magánfelhő esetén a SZEÜSZ szolgáltatóval szembeni követelmények:

- *Több fizikai helyszín (megrendelő több létesítménye) esetén a SZEÜSZ szolgáltatónak biztosítania kell megbízható (igény vagy szükség esetén dedikált) vonalat a különböző fizikai helyszínek közötti (védett) kommunikációra (ha technikai sajátosság, vagy nyilvánvaló gazdaságossági szempont mást nem indokol, a szükséges hálózati feltételeket a Nemzeti Távközlési Gerinchálózat igénybevételével kell megteremteni);*

- *A SZEÜSZ a szolgáltatást igénybe vevő igénye szerinti helyszínen (vagy több helyszínen) alakítja ki a magánfelhő infrastruktúrát, a szolgáltatónak alkalmazkodnia kell a földrajzi helyhez, környezethez, e feltételek között kell megfelelően üzembiztos és biztonságos informatikai környezetet létrehoznia;*

- *A SZEÜSZ szolgáltatónak biztosítania kell, hogy a felhőhasználó hatóságnak lehetősége legyen erős ún. demilitarizált zóna (DMZ) kialakítására, amelyben az elhelyzett hostoknak csak jól szabályozott, korlátozott kapcsolatban szabad lenniük a belső hálózatba tartozó gépekkel, biztosítandó a magánfelhő erőforrásainak külső támadások elleni védelmét. A kommunikáció más hostokkal a DMZ-n belül és a külső hálózatba viszont engedélyezett. Ez teszi lehetővé, hogy a DMZ-n belüli hostok szolgáltatást nyújthassanak mind a belső, mind a külső hálózatba, ami a hagyományoshoz hasonló biztonsági szintet eredményez (és külön, megfelelő mechanizmusokkal tovább erősítve a nagyobb érzékenységű adatok védelmét);*

- *A SZEÜSZ szolgáltatónak biztosítania kell, hogy az ügyfélnek lehetősége legyen redundáns megoldások használatára mind a kommunikáció, mind pedig az igénybevett szolgáltatások tekintetében.*

A külső szolgáltatásként megvalósított magánfelhő esetén a SZEÜSZ szolgáltatóval szembeni követelmények:

- *A SZEÜSZ szolgáltatónak biztosítania kell megbízható (igény esetén dedikált) vonalat (ha technikai sajátosság, vagy nyilvánvaló gazdaságossági szempont mást nem indokol, a szükséges hálózati feltételeket a Nemzeti Távközlési Gerinchálózat igénybevételével kell megteremteni);*
- *A SZEÜSZ szolgáltatónak törekednie kell arra, hogy a szolgáltatást igénybe vevő szervezet pontos információkat kaphasson a szerverek és infrastrukturális eszközök fizikai helyéről;*
- *A SZEÜSZ szolgáltatónak garantálnia kell fizikai és logikai védelmi intézkedésekkel, hogy kizárólag a magánfelhő használója (és annak ügyfelei) férnek hozzá a szolgáltató telephelyén kialakított informatikai infrastruktúrához, az erőforrásokat csak az erre kijelölt eszközparkból biztosítja (a fizikai és védelmi intézkedések további lebontási szintje függ a szolgáltatási modelltől);*
- *A SZEÜSZ szolgáltatónak gondoskodnia kell a szolgáltatást igénybe vevő szervezettel való kommunikáció védelméről, és a magánfelhő infrastruktúra biztonsági határainak védelméről;*
- *A SZEÜSZ szolgáltatónak biztosítania kell, hogy az ügyfélnek lehetősége legyen redundáns megoldások használatára mind a kommunikáció, mind pedig az igénybevett szolgáltatások tekintetében.*

3.4.2. Közösségi felhő

A közösségen belül egy vagy több szervezet lehet a tulajdonos, a kezelő, üzemeltető, de lehet harmadik fél is, vagy a kettő kombinációja. A felhő létesítése történhet a telephelyen vagy attól távol is.

Helyszíni közösségi felhő esetén:

- *A SZEÜSZ szolgáltatónak a résztvevő szervezetek közötti tényleges függéseket meg kell ismernie az esetleges hibákból eredő következmények kezelése érdekében (ide tartozik a résztvevő szervezetek egymás számára biztosított szolgáltatásainak üzem- és információbiztonsága);*
- *Több fizikai helyszín (szolgáltatást igénybe vevő szervezetek több létesítménye) esetén a SZEÜSZ szolgáltatónak biztosítania kell megbízható (igény esetén dedikált) vonalat a különböző fizikai helyszínek közötti (védett) kommunikációra (ha technikai sajátosság, vagy nyilvánvaló gazdaságossági szempont mást nem indokol, a szükséges hálózati feltételeket a Nemzeti Távközlési Gerinchálózat igénybevételével kell megteremteni);*
- *A SZEÜSZ szolgáltatónak biztosítania kell, hogy az ügyfélnek lehetősége legyen*

redundáns megoldások használatára mind a kommunikáció, mind pedig az igénybevett szolgáltatások tekintetében.

Külső szolgáltatásként megvalósított közösségi felhő esetén:

- *A SZEÜSZ közösségi szolgáltatónak biztosítania kell megbízható vonalat (ha technikai sajátosság, vagy nyilvánvaló gazdaságossági szempont mást nem indokol, a szükséges hálózati feltételeket a Nemzeti Távközlési Gerinchálózat igénybevételével kell megteremteni);*
- *a SZEÜSZ szolgáltatónak meg kell határoznia a résztvevő szervezetek (mint közösség) közötti erőforrás-megosztás szabályait;*
- *A SZEÜSZ szolgáltatónak törekednie kell arra, hogy a szolgáltatást igénybe vevő szervezet pontos információkat kaphasson a szerverek és infrastrukturális eszközök fizikai helyéről;*
- *A SZEÜSZ szolgáltatónak garantálnia kell fizikai és logikai védelmi intézkedésekkel, hogy kizárólag a közösségi felhő felhasználója (és annak ügyfelei) férnek hozzá a szolgáltató telephelyén kialakított informatikai infrastruktúrához, az erőforrásokat csak az erre kijelölt eszközparkból biztosítja (a fizikai és védelmi intézkedések további lebontási szintje függ a szolgáltatási modelltől);*
- *A SZEÜSZ szolgáltatónak biztosítania kell, hogy az ügyfélnek lehetősége legyen redundáns megoldások használatára mind a kommunikáció, mind pedig az igénybevett szolgáltatások tekintetében.*

3.5. Szolgáltatási modell szerinti biztonsági követelmények

Az egyes felhőalapú szolgáltatási modellek esetén a felelősségek megoszlanak a szolgáltató és a szolgáltatást igénybe vevő között. Ez érinti a funkcionalitással kapcsolatos feladatokat, és az adott funkcionális rétegben a biztonsági intézkedések megvalósítását is.

A konkrét biztonsági támogatási feladatokat a szolgáltatási szabályzatban (vagy SLA-ban) kell rögzíteni, hiszen sokminden függ a telepítési modelltől és a szolgáltatás tényleges megvalósításától, az adatvédelmi követelményektől. A szolgáltatási szabályzatban és/vagy SLA-ban kell a SZEÜSZ informatikai háttér szolgáltató és az igénybe vevő közigazgatási hatóság által közös felelősséggel végzendő feladatokat meghatározni, megadva az ezekhez szükséges szerepköröket is. A fő szempont az információvédelem és az informatikai rendszer biztonsága, ennek megvalósításához járul hozzá teljes vagy részleges mértékben a szolgáltató a különböző szolgáltatási kategóriákban. Teljes felelősségi kör esetén a SZEÜSZ szolgáltatónak az informatikai háttérszolgáltató rendszer egészének megbízható és biztonságos működése szempontjából teljes felelőssége van. Részleges felelősségi kör esetén a SZEÜSZ szolgáltatóra háruló felelősség az informatikai rendszer egészének megbízható és biztonságos működése szempontjából részleges.

A részleges felelősségi kör esetében a szolgáltatási szabályzatban vagy SLA-ban foglaltak az irányadóak, ekkor osztott a felelősség az igénylő szervezettel a teljes rendszer biztonságára nézve.

3.5.1. Adatvédelmi, információbiztonsági megfelelőség

- *A SZEÜSZ szolgáltatónak az elektronikus ügyintézés során a jogszabályokban előírt védelmet kell biztosítania a felhőben tárolt és kezelt adatokra, azok biztonsági paramétereinek megfelelő mechanizmusokat kell alkalmaznia a szolgáltató által felügyelt infrastruktúra rétegekben értelmezhető elemeire;*

- *Közzé kell tennie vagy a SZEÜSZ-t igénybe vevő ügyfél számára biztosítania kell az adatkezeléssel kapcsolatos mechanizmusait és az adatvédelmi jogszabályoknak való megfelelőséget. Egyértelművé és megismerhetővé kell tennie az adatokhoz való hozzáférés lehetőségeit, az adatok őrzése, tárolása, továbbítása, használata és megsemmisítése során követett eljárásokat és azok garanciáit;*

- *A SZEÜSZ szolgáltatónak meg kell felelnie a biztosított szolgáltatással kapcsolatos adatmegőrzési jogszabályoknak (például a naplók előírt időtartamig történő megőrzése). A megfelelést az adatkezelési mechanizmusok ismertetésével a vonatkozó dokumentációkban szerepeltetni kell;*

- *A SZEÜSZ szolgáltatónak gondoskodnia kell az igénybe vevő hatóság olyan adatvédelmi igényéről, amely az érzékeny és nem érzékeny adatok elkülönítését írja elő, ez a funkció szükségszerűen a szolgáltatás részét képezi;*

- *A SZEÜSZ informatikai háttér szolgáltatását végző szolgáltatónak tilos bármilyen adatfeldolgozást végeznie saját vagy kereskedelmi célra (például hirdetések vagy statisztikai adatok előállítása), ezt az adatvédelmi nyilatkozatban rögzíteni kell. A rendszer monitorozásával kapcsolatos adatok kezeléséről, naplóadatok hatósági eljárásban való kiadásáról külön kell rendelkezni;*

- *A SZEÜSZ szolgáltatónak eljárásokat kell kidolgoznia a rendszerében tárolt adatok megbízható törlésére, ideértve az igénybe vevő hatóság általi kérésre történő törlést, vagy egyéb, normál szolgáltatási munkamenetből eredő maradvány információk törlését (pl ideiglenes fájlok, szolgáltatási szabályzatban megállapított metaadat őrzési idők lejárata utáni törlést).*

3.5.2. Szervezeti szintű alapfeladatok

- *A SZEÜSZ szolgáltatónak érvényes informatikai biztonsági szabályzattal kell rendelkeznie;*

- *A szolgáltatónak átlátható és – a telepítési és szolgáltatási modelltől függő mértékben – fejlesztési (tervezési, specifikációs, megvalósítási), dokumentálási, életciklus-támogatási (konfigurálási, frissítési, patchelési, verziókövetési), tesztelési, üzemeltetési, hibakövetési, monitorozási szabályokat kell kidolgoznia;*

- *A SZEÜSZ szolgáltatónak dokumentált módon kell az eljárásrendi és technikai biztonsági intézkedéseket megvalósítania. Az igénybe vevő hatóságot érintő bárminemű dokumentációmódosításról haladéktalanul tájékoztatásta kell.*

3.5.3. Rendszer- és szolgáltatásbeszerzés

- *A SZEÜSZ szolgáltatónak a vonatkozó jogszabályoknak megfelelő eljárásrend alapján kell a szolgáltatás alapjául szolgáló informatikai erőforrásokat beszerezni;*
- *A SZEÜSZ szolgáltatónak az általa biztosított szolgáltatási rétegnek megfelelően gondoskodnia kell a megfelelő licenszelésről (jellemzően SaaS esetén minden szoftverlicencről, PaaS esetén részben, IaaS esetén pedig ez a feladat elsősorban az igénybe vevőre hárul), nem felhőalapú kialakítás esetén pedig a felhasznált operációs rendszerek, adatbáziskezelők, tartalomkezelők stb. jogtiszta felhasználásáról.*

3.5.4. Kockázatelemzés

Az adatokkal és az adatfeldolgozással kapcsolatos kockázatok felmérése felhasználói felelősség. A SZEÜSZ szolgáltatónak az általa vállalat szolgáltatási szint és minőség vonatkozásában van kockázatfelméréséi és értékelési kötelezettsége (a változó körülmények, új technológiák alkalmasak-e a vállalt szolgáltatási szint nyújtására, a nem teljesítésnek milyen kockázatai vannak a szolgáltatóra nézve stb.).

3.5.5. Tervezés

A SZEÜSZ szolgáltató feladatköre az információbiztonsági tervezésre SaaS szolgáltatás esetén teljes körű, de a szolgáltatási szabályzatban az igénybe vevő hatóság hozzájárulását is rögzíteni kell. A másik két modellben, valamint nem felhő alapú kialakításban a biztonsági tervezésnek az alapinfrasturktúra elemeire kell kiterjednie.

3.5.6. Személyzettel kapcsolatos biztonság

A SZEÜSZ szolgáltatónak az emberi erőforrás megbízhatóságának biztosítása érdekében a háttérszolgáltatást biztosító szolgáltatói állomány tekintetében gondoskodnia kell a vonatkozó jogszabályokban rögzített megfelelőségi követelmények teljesítéséről (például érzékeny adatok feldolgozását végző rendszerhez kik kaphatnak fizikai és logikai hozzáférést).

3.5.7. Tudatosság és képzés

A SZEÜSZ szolgáltatónak a szakembereit az alkalmazott technológiák naprakész ismerete és a vonatkozó jogszabályok, eljárásrendi intézkedések szabályos betartása érdekében folyamatosan képeznie kell.

3.5.8. Fizikai védelem

A SZEÜSZ szolgáltató teljes mértékben felelős a központi erőforráshardverek, géptermek és egyéb létesítmények fizikai biztonságának fenntartásáért.

3.5.9. Konfigurációkezelés

- *SaaS esetén a SZEÜSZ szolgáltató teljes mértékben felelős az általa szolgáltatott erőforrások konfigurációmenedzsmentjéért, ideértve a förmvereket, hardverkomponensek listáit, szoftverek verzióinak nyomon követéséért.*

- *PaaS és IaaS, illetve nem felhőalapú kialakítás esetén a felelősség az alkalmazói réteg szoftvereire nem terjed ki.*

3.5.10. Üzletmenet folytonosságának tervezése

A SZEÜSZ szolgáltatónak a szolgáltatott erőforrások tekintetében kidolgozott üzletmenet-folytonossági tervvel kell rendelkeznie, igazolandó az igénybe vevő hatóságok számára az állított rendelkezésre állást (szükség szerinti redundancia biztosításával) és teljesítményt.

3.5.11. Karbantartás

- *SaaS esetén a SZEÜSZ szolgáltató felelősségei közé tartozik az üzemeltetési, karbantartási feladatok elvégzése: mentések, rendszerkarbantartás, biztonsági frissítések, hardverek energiagazdálkodása, hardver- és firmware-frissítések végrehajtása;*

- *PaaS esetén a szolgáltató felelőségi körébe tartozik a platformkomponensek kiválasztása, telepítése, karbantartása és üzemeltetése, alap hardver infrastruktúra karbantartása;*

- *IaaS és nem felhőalapú kialakítás esetén a szolgáltató felelőségi körébe tartozik a megfelelően kialakított operációs rendszer image-k és szolgáltatások biztosítása, redundáns tárolás, kriptográfiai szolgáltatás, tűzfalak, monitorozás, szükség esetén forensic analízis, incidenskezelés, igény alapú automata virtuális gép indítás és leállítás stb., azaz a hypervisori és fizikai réteg karbantartása.*

3.5.12. Adathordozók védelme

- *A SZEÜSZ szolgáltatónak gondoskodnia kell az általa kezelt hardver infrastruktúrán lévő adatok hordozóinak biztonságos kezeléséről (központi gépteremben lévő adathordozók cseréje, meghibásodása, szakszerviz stb);*

- *A szolgáltatónak meg kell felelnie a vonatkozó szabályoknak, a szolgáltatási szabályzat és/vagy SLA szerinti megállapodásnak a tekintetben, hogy kiadhatja-e a SaaS szolgáltatás alapinfrastruktúráját képező hardvert javításra, és ha igen,*

akkor milyen törlési eljárások után;

3.5.13. Azonosítás/hitelesítés és hozzáférésellenőrzés

A SZEÜSZ szolgáltatónak a szolgáltatási szabályzatban vagy SLA-ban publikálnia kell

- *az általa biztosított infrastruktúrában alkalmazott azonosítási, hitelesítési és hozzáférésellenőrzési eljárási mechanizmusokat;*
- *az igénybe vevő hatóságok ügyfelei által alkalmazható eszközöket az alkalmazásfiókok és ügyfélengedélyek adminisztrálásához.*

3.5.14. Naplózás és ellenőrizhetőség

- *A naplózásnak és ellenőrizhetőségnek ki kell terjednie minden fontos hardver, hálózati és szoftveres erőforráshoz való (fizikai és virtuális) hozzáférésre;*
- *A SZEÜSZ szolgáltatónak biztosítania kell, hogy a szolgáltatást igénybe vevő hatóság hozzáférjen az őt érintő rendszer-, biztonsági és tevékenységi naplókhoz, a felhasználó által olvasható formátumban;*
- *Az érzékeny adatokat tartalmazó naplóállományok bizalmassági védelméről a szolgáltatónak gondoskodnia kell;*
- *A naplóállományok sértetlenségét és megváltoztathatatlanságát a szolgáltatónak biztosítania kell;*
- *SaaS esetén a SZEÜSZ szolgáltatónak biztosítania kell a rendszer mellett a szolgáltatás használatával kapcsolatos naplózást és ellenőrizhetőséget is;*
- *PaaS esetén a SZEÜSZ szolgáltatónak az operációs rendszerek, virtuális gépek használatára vetítve kell biztosítania naplózást;*
- *IaaS és nem felhőalapú kialakíts esetén az operációs rendszerek, adatbáziskezelők, tartalomkezelők stb. vonatkozásában kell biztosítania a naplózást.*

3.5.15. Rendszer, kommunikáció és információ védelme, sértetlensége

- *Bizalmassági biztonsági követelményt igénylő feldolgozásnál a SZEÜSZ szolgáltatónak gondoskodnia kell a kommunikációs csatornán átfolyó, illetve a tárolt adatok illetéktelenek általi megismerése elleni védelméről. Az erre alkalmazott technológia feleljen meg a legszélesebb körben alkalmazott módszereknek (SSH, SFTP, SSL/TLS, Kerberos);*
- *Sértetlenségre érzékeny adatfeldolgozásnál a SZEÜSZ szolgáltatónak gondoskodnia kell a kommunikációs csatornán átfolyó, illetve a tárolt adatok illetéktelenek általi módosítása elleni védelméről, a legszélesebb körben*

alkalmazott technológiákkal (SHA, CRC, Reed-Solomon);

- *Titkosítás használata esetén a SZEÜSZ szolgáltatónak a kriptográfiai kulcsok menedzselésére, védelmére, az azokhoz való hozzáférési szabályokra vonatkozó eljárásrendet kell kidolgoznia és alkalmaznia, igazodva az alkalmazott kulcsok jellegéből következő technikai követelményekhez (például nyilvános kulcsú titkosítás esetén a kulcspároknak megfelelő kezelése, szimmetrikus kulcsú titkosításnál a kulcskiosztás bizalmassága, az ezeket garantáló technikai eszközök igénybevételével);*

- *A SZEÜSZ szolgáltatónak gondoskodnia kell a biztosított szolgáltatás elvártak szerinti működéséről (a szolgáltatás funkcióinak működését illetéktelen nem módosította, a szolgáltató felelősségi körébe eső beállításokat illetéktelen nem állította át); ehhez kártékony szoftvereket és illetéktelenek általi behatolásokat elhárító biztonsági határvédelmi megoldásokat, szükség esetén pedig a megfelelő incidenskezelési és forensic analízisre szolgáló eszközöket kell alkalmaznia;*

- *Virtuális gépek alkalmazása esetén a SZEÜSZ szolgáltatónak biztosítania kell a virtuális gépek más VM-ek felől, a fizikai hosztról és hálózat felől érkező támadások elleni védelmét.*

- *SaaS esetén a szolgáltatónak nyomon kell követnie a hálózati erőforrásokhoz, alkalmazásokhoz és adatokhoz való hozzáféréseket. Az alkalmazási szintig elérő sebezhetőségek esetén az alkalmazásspecifikus védelmi megoldásokat is biztosítania kell (például levelező program/spamszűrő, böngésző biztonsági frissítése);*

- *PaaS és Iaas, valamint nem felhő alapú kialakítás esetén a réteghez tartozó hálózati erőforrásokhoz való hozzáféréseket nyomon kell követnie. Az alkalmazói szoftverek alatti rétegeket érintő sebezhetőségi pontokat megfelelő eszközökkel védenie kell (tűzfalak, böngészők frissítése stb.);.*

- *Biztosítani kell, hogy a PaaS környezetben fejlesztett alkalmazás biztonságosan futtatható üzemmódra konfigurált legyen (például titkosítás kliens-szerver kommunikációban), és integrálható legyen a fejlesztett alkalmazást igénybe vevő hatóság meglévő technikai biztonsági intézkedéseivel (azonosítás, hitelesítés, engedélyezési folyamatok). Az erre szolgáló technikai eszközök a széles körben használt de facto szabványoknak megfelelőek legyenek (SSH, SFTP, SSL/TLS, Kerberos).*

3.5.16. Reagálás a (biztonsági) eseményekre

- *A SZEÜSZ szolgáltatónak monitorozó rendszert kell üzemeltetnie, és biztonsági incidens detektálása esetén értesítést kell küldenie az ügyfélnek;*

- *A SZEÜSZ szolgáltatónak a szolgáltatási szabályzatban meghatározott időn belül ki kell vizsgálnia a szolgáltatás teljesítményével (nem megfelelő válaszidők, nem elég gyors erőforrás igénylési reagálás stb.) kapcsolatos jelenségeket, és gondoskodnia*

kell arról, hogy a szolgáltatás nyújtására alkalmas szolgáltatási színvonalat fenntarsa;

- *A SZEÜSZ szolgáltatónak rendelkezésre kell állnia külső auditálási ellenőrzések lefolytatására, a privilegizált használattal kapcsolatos rendszerhasználat dokumentálásának ellenőrzésére, az eseménykezelési eljárások illetékes hatóság általi ellenőrzésére, az erőforrások illegális vagy nem megfelelő használatának gyanúja esetén az eljárás során az eljáró hatósággal, illetve a szolgáltatás igénybevőjével együtt kell működnie.*

3.6. Adatmigrálás a szolgáltató és az igénybevevő infrastruktúrája között

A fontos alkalmazások és adatok szervezettől a SZEÜSZ szolgáltatójának infrastruktúrájára való átvitelének vonatkozásában nem elsősorban a technikai, hanem a biztonsági és adatvédelmi kérdések jelentik a legfőbb megoldandó problémát. A SZEÜSZ szolgáltatónak garanciákat kell adnia és mechanizmusokat kell biztosítania az adatok és egyéb logikai erőforrások biztonságos

- *fogadására,*
- *a szolgáltatás indítására,*
- *a szolgáltatás felmondása esetén elvégzendő lépésekre:*
  - *fizikai és elektronikus hozzáférések visszavonása;*
  - *a felhasználó hatóság adatainak és erőforrásainak (dokumentumainak, egyéb kapcsolódó szoftvereinek) visszaszolgáltatása;*
  - *adatok, programok, mentések bizonyított és visszavonhatatlan törlése a szolgáltató rendszeréből a dokumentált visszaszolgáltatás után;*
  - *naplók és egyéb nyomon követési, monitorozási adatok átadása és igazolt átvétele a később felvetődő vitás esetek megelőzésére.*

A SZEÜSZ szolgáltató irányában támasztott adatkezelési, biztonsági és bizalmassági követelményekből következően a szolgáltató nem migrálhat tovább más felhő- vagy hagyományos háttérszolgáltatóhoz semmilyen, a szolgáltatását igénybe vevő hatóság vagy szervezet által rendelkezésére bocsátott IT-értéket.

4. Hagyományos informatikai központok

Amennyiben a SZEÜSZ szolgáltatója saját infrastruktúrán valósítja meg a szolgáltatást, akár felhő-jellegű, akár többrétegű funkcionális kiépítést és szolgáltatási modellt alkalmazva, az informatikai háttér műszaki kialakításakor a széles körben elterjedt nemzetközi és hazai gyakorlatot kell követnie. A szolgáltatás minőségi paramétereinek (folyamatosság, rendelkezésre állás, robusztusság stb.) biztosítása érdekében kerülni kell minden egyedi, ideiglenes, nem rendszerbe illő vagy ad-hoc megvalósítást, amelyek a szervizelést, a szükség esetén felmerülő strukturális átalakítást, valamint a szakszemélyzet képzését és fluktuációjának kezelését nehézzé vagy kockázatossá teszik.

4.1. A többrétegű architektúra modellje

Napjainkban általános a többrétegű architektúra szerinti felépítés is, amennyiben nem szolgáltatásorientált architektúra kerül kiépítésre. A réteg egy funkcionálisan elkülönített hardver és szoftver komponenst jelent, a legtisztább esetben dedikált erőforrásokon üzemeltetve. Ebből eredően az ideális működési környezet a több, eltérő funkcionalitású szerverre épített architektúra.

A következő rétegeket különböztetjük meg:

- *A megjelenítési réteg (felhasználói felület, kliens, user interface) felelős a felhasználói felületért és a felhasználóval való kapcsolattartásért, az architektúra legtetején helyezkedik el. A kliens felületnek felhasználóbarátnak, ugyanakkor robusztusnak kell lennie.*

- *A távoli elérést kiszolgáló réteg felelős a felhasználói felülettel való kapcsolattartásért. A kliens kéréseit továbbítja az alkalmazási réteg felé, illetve az onnan érkezett válaszokat küldi vissza a kliensnek. Alapvetően ez a réteg képezi a választóvonalat a szervezet megbízható belső hálózata és a megbízhatatlannak ítélt külső hálózat (például az internet) között.*

- *Az alkalmazási réteg (alkalmazáslogika, üzleti logika) felelős az alkalmazás által megfogalmazott feladatok végrehajtásáért, az egy szinttel lejjebb elhelyezkedő adatbázis rétegtől a szükséges adatok megszerzéséért, illetve ezen adatok kezelésének vezérléséért. Ez a réteg a biztonságos belső hálózatban található, feladatát egy vagy több alkalmazásszerver látja el.*

- *Az adatbázis-réteg az adatok fizikai eléréséért, feldolgozásáért felelős. E réteg feladata például az adatbázis állományok nyitása, zárása, új adat felvitele, törlése, módosítása, indexek kezelése, zárolási konfliktushelyzetek feloldása. Ez a réteg az adatok alkalmazásoktól független tárolásáért felelős. Ebben a rétegben kaphatnak helyet az adatbázisok, adatbázis-szerverek, file-szerverek, különböző háttértárak.*

- *Az operációs rendszer rétege a fenti rétegek és a fizikai hardver közötti*

kapcsolatot biztosítja.

4.2. Kialakítandó környezetek

Célszerű több, egymástól eltérő funkcionalitású informatikai környezet kialakítása. Az egyes környezetek hasonló szolgáltatással épülnek ki, csak méretbeli, illetőleg rendelkezésre állás-beli különbség van közöttük. Ennek érdekében a szolgáltatónak törekednie kell a következő kialakítási elvek érvényesítésére:

4.2.1. Éles üzemi környezet

- *adatbázis- és alkalmazásszerverek;*
- *gyorsító tárak, belső ramdiskeken és/vagy SSD-tárolókon megvalósítva;*
- *rendszerkritikus és adminisztratív, illetve felügyelő szolgáltatások dedikált erőforrásokkal való biztosítása (független e-mail-szerver és felügyeleti rendszer, autentikáció kezelése stb.);*
- *redundáns, robusztus és elosztott tárhelyszolgáltatás, NAS architektúra és/vagy SAN-hálózatba kötött tárolók;*
- *nagysebességű, felügyelt, trönkvonalakon megfelelően méretezett kapacitású, fizikailag védett adatátviteli hálózat;*
- *klimatizált gépterem, stabil és szünetmentes áramellátás;*
- *földrajzilag is redundáns kiépítés.*

4.2.2. Tesztkörnyezet

Tesztkörnyezet kialakítása az alkalmazásokban végrehajtott javítások, módosítások, kiegészítések, továbbá a jövőbeli továbbfejlesztések működésének ellenőrizhetősége miatt szükséges. Kiépítettsége funkcionálisan megegyezik az éles üzemi környezetével, de teljesítményben, valamint rendelkezésre állás tekintetében szerényebb képességekkel bír.

4.2.3. Végellenőrzési környezet

Ebben a környezetben történik, a sikeres teszteket követően, az éles üzemi környezetbe telepítendő programverzió utolsó ellenőrzése. A tesztkörnyezet számára fenntartott hardvereken üzemel.

4.3. A kialakítás javasolt dedikált elemei

- *Adatbázisszerverek*

- *Alkalmazásszerverek*
- *Gyorsítótár-szerverek*
- *Menedzsment-szerver*
- *E-mail-szerver*
- *Rackszekrények*
- *Tárolók + SAN bővítés*
- *Hálózati eszközök, kiegészítő eszközök*
- *Betáplálás, klíma, belső kábelezés*
- *Mentőrendszer*
- *Mentőszerver*
- *Biztonsági eszközök*
- *Tűzfalak, IPS*

4.4. Üzemeltetési támpontok

Gazdaságossági szempontok csak olyan mértékig érvényesíthetők, hogy a SZEÜSZ szolgáltató garantálni tudja a szolgáltatás elvárt minőségi színvonalát, amelyért teljeskörű felelősséggel tartozik.

Javasolt az Információbiztonsági Fórum által kidolgozott „bevált gyakorlatok szabványa" (Standard of Good Practice vagy SoGP), a következő kérdések kezelésére:

- *kockázatértékelések (javasolt az ISO/IEC 27005 vagy egyéb konkrét és megfelelő kockázatértékelési módszertan);*
- *fizikai és környezeti biztonság;*
- *humánerőforrás-biztonság;*
- *kommunikáció- és műveletirányítás;*
- *a hozzáférés-vezérlésre vonatkozó szabványos intézkedések;*
- *információs rendszerek beszerzése, fejlesztése és fenntartása;*
- *információbiztonsági kezelés;*
- *intézkedések az információs rendszerek olyan rendszerbiztonsági eseményeinek orvoslására és csökkentésére, amelyek a feldolgozott személyes adatoknak*

megsemmisítését vagy véletlen elvesztését, megváltoztatását, jogosulatlan nyilvánosságra hozatalát vagy az ahhoz való jogosulatlan hozzáférést eredményeznék;

- *a számítógépes hálózat biztonsága (javasolt az ISO/IEC 27033 vagy a bevált gyakorlatok szabványa).*

4.5. Funkcionális biztonsági követelmények

Amennyiben a rendszer üzemeltetése különböző feladatköröket tesz szükségessé, úgy ezekhez különböző hozzáférési szinteket kell létrehozni a minimális üzemeltetési jogosultság (a lehető legkevesebb jogosultság) elvének megfelelően.

Az esetlegesen nyilvánosan elérhető funkciókat egyértelműen el kell választani a rendszer üzemeltetésére szánt funkcióktól. A hozzáférés-vezérlés nem akadályozhatja a rendszer rendelkezésre álló információk elérhetőségét.

4.5.1. Az alkalmazási szint biztonsága

A rendszernek megfelelően védettnek kell lennie az ismert biztonsági rések és az azok elleni „exploit” típusú támadások ellen. Ebből a célból többek között védelmet kell nyújtania az olyan kódbeszúrásos támadások (injections) ellen, mint a strukturált lekérdezési nyelv (Structured Query Language, SQL) alapján történő lekérdezések, a könnyű címtárelérési protokoll (Lightweight Directory Access Protocol, LDAP) alapján történő lekérdezések, az XML Path nyelv (XPath) alapján történő lekérdezések, az operációs rendszerek parancsai vagy programargumentumok. Ebből a célból alapkövetelmény, hogy:

- *valamennyi felhasználó által megadott bemenő paramétereket ellenőrzik;*
- *az ellenőrzés legalább a szerveroldali logikán keresztül történjen;*
- *valamennyi értelmezőprogram egyértelműen válassza szét a nem megbízható adatokat a parancstól vagy lekérdezéstől.*

A rendszernek szigorú hitelesítéssel és munkamenet-kezeléssel kell rendelkeznie, amely szerint alapkövetelmény, hogy:

- *a hitelesítő adatok a tárolás idején mindig védelem alatt állnak kivonatolással (hashing) vagy titkosítással. Csökken annak kockázata, hogy valaki "pass-the-hash" támadást alkalmazva hitelesít;*
- *a hitelesítő adatokat nem lehet kitalálni vagy felülírni gyenge fiókkezelési funkciók révén (pl. fiók létrehozása, jelszó módosítása, jelszó helyreállítása, gyenge munkamenet-azonosítók (session ID-k));*
- *a munkamenet (session) azonosítói és a munkamenet-adatok nem jelennek meg a szolgáltatás külső oldalán (például URL-ben);*

- *a munkamenet azonosítóit nem veszélyeztetik a munkamenet-rögzítéses támadások;*
- *a munkamenet-azonosítók korlátozott idejűek, ami biztosítja, hogy a felhasználók ne maradjanak bejelentkezve;*
- *a munkamenet-azonosítókat sikeres bejelentkezés után nem használják fel újra;*
- *a jelszavakat, munkamenet-azonosítókat és egyéb hitelesítő adatokat csak titkosított protokollon (SSH, SSL, TLS) keresztül küldik meg;*
- *a rendszer adminisztrációs része is védelem alatt áll. Amennyiben egytényezős hitelesítés (SFA) védi, akkor a jelszónak minimum tíz karakterből kell állnia, beleértve legalább egy betűt, egy számot és egy speciális karaktert. Választási lehetőségként a kéttényezőjű hitelesítés is használható. Egytényezős hitelesítés esetén a rendszer adminisztrációs részéhez a szolgáltatón kívülről (pl. interneten keresztül) való hozzáférésre vonatkozó kétlépcsős ellenőrzési mechanizmus szükséges.*

Megfelelő biztonsági konfiguráció létrehozása szükséges, amely szerint alapkövetelmény, hogy:

- *valamennyi szoftverösszetevő naprakész legyen, beleértve az operációs rendszert, a webalkalmazás-kiszolgálót, az adatbázis-kezelő rendszert (DBMS), az alkalmazásokat, valamint valamennyi kódkönyvtárat;*
- *az operációs rendszer és a web/alkalmazás-kiszolgáló, valamint egyéb alkalmazások szükségtelen szolgáltatásai le vannak tiltva, el vannak távolítva vagy nincsenek telepítve;*
- *a hibakezelés kialakítása megakadályozza, hogy a veremkivonatokon és egyéb túlságosan informatív hibaüzeneteken keresztül érzékeny információk szivárogjanak ki;*
- *a fejlesztési keretek és könyvtárak biztonsági beállításai a bevált gyakorlatoknak megfelelően vannak konfigurálva.*

4.5.2. Hálózatbiztonság

A rendszerek tűzfallal való védelme szükséges. Amennyiben a tűzfal legfontosabb frissítései és javításai nyilvánosak lesznek, úgy az ilyen frissítéseket és javításokat ennek megfelelően a SZEÜSZ szolgáltató telepíti.

A rendszer bemenő és kimenő forgalmának jellemzőit a szolgáltatónak vizsgálnia és naplóznia kell a tűzfalszabályoknak megfelelően. A tűzfalszabályoknak meg kell tagadniuk minden olyan forgalmat, amely nem szükséges a rendszer biztonságos használatával és üzemeltetésével

kapcsolatosan.

A kialakított architektúrában megfelelően védett hálózati szegmenseknek kell üzemelniük, ahol a funkcionálisan eltérő szegmensek egymástól el vannak választva (VLAN). A helyi hálózat (LAN) szükséges biztonsági intézkedései körében a használaton kívüli kapcsolóportok legyenek letiltva, az ütközőzóna egy kijelölt virtuális helyi hálózaton (VLAN)/helyi hálózaton (LAN) legyen található, és nem lehet engedélyezett Layer-2 trönkkapcsolat a felesleges portokon.

4.5.3. Operációs rendszer és alkalmazásszerver biztonsága

Az alkalmazásoknak a futtatáshoz szükséges jogosultságok legalacsonyabb szintjével kell futniuk. Amennyiben az operációs rendszer, az alkalmazás futtatórendszerei, a szervereken futtatott alkalmazások vagy kártevőirtók legfontosabb frissítései és javításai nyilvánosak lesznek, úgy az ilyen frissítéseket és javításokat ennek megfelelően a SZEÜSZ szolgáltató telepíti.

4.6. Szolgáltatás teljesítménye és minősége

4.6.1. Skálázhatóság

A rendszert úgy kell megtervezni és létrehozni, hogy annak minden lényeges komponense skálázható legyen. Tehát az üzemeltetés során, a rendszer kapacitásának minimális erőfeszítéssel, a rendszer felépítésének módosítása nélkül, a terheléssel arányosan növelhetőnek kell lennie.

Ezért kiemelt figyelmet kell fordítani:

- *a tranzakciószám emelkedése;*
- *a tranzakciók bonyolultságának növekedése;*
- *a felhasználói szám növekedése;*

esetén a szükséges intézkedések megtételére.

4.6.2. Bővíthetőség, módosíthatóság

A rendszer tervezése és kialakítása során figyelembe kell venni a módosíthatóság és kiterjeszthetőség szempontjait, mivel az elvárt funkcionalitásban változások lehetnek a jogszabályok, és az igazgatási folyamatok módosulása okán.

- *Módosíthatóság: a rendszer meglévő funkcionalitásának, valamint az igazgatási folyamatoknak az egyszerű megváltoztathatósága*
- *Kiterjeszthetőség: a rendszerhez könnyedén lehessen új funkciókat, folyamatokat*

hozzáadni.

4.6.3. Megbízhatóság

A rendszer megbízhatóságának szempontjai a következők:

- *Rendelkezésre állás: az éves megengedett maximális üzemkiesésbe bele kell számolni a karbantartás, rendszerfrissítés, adatmentés, archiválás stb. céljából tervezett leállások időtartamát is, amennyiben ez szolgáltatás-kieséssel jár együtt;*
- *Robusztussága: rendszer alkotóelemeiben történő bárminemű meghibásodás nem befolyásolhatja negatívan a többi alkotóelemének folyamatos működését, továbbá egy új interfészen kapcsolódó új rendszer illesztése nem lehet negatív hatással a működő rendszerre;*
- *Adatintegritás és konzisztencia: a rendszernek garantálnia kell a rajta keresztül továbbított, illetve benne tárolt adatok integritását és konzisztenciáját. Az adatbázisokban és az üzenetfeldolgozó modulokban olyan megoldásokat kell alkalmazni, amelyek biztosítják, hogy a tárolt és továbbított, egymással összefüggő adatok között az összefüggések ellentmondásmentesek legyenek.*

4.6.4. Naplózásra, auditra vonatkozó követelmények

A szolgáltatási rendszer naplózási mechanizmusának és a naplók tárolásának meg kell felelniük a mindenkor hatályos adatkezelési, adatvédelmi szabályozásnak. A rendszernek naplóznia kell minden felhasználói és adminisztrátori tevékenységet is a rendszerben elvégzett műveletek nyomon követhetősége érdekében. A naplóban az elvégzett műveletekkel együtt tárolni szükséges a végrehajtó személy beazonosíthatóságához szükséges adatot vagy adatokat, valamint a műveletvégzés idejét és egyéb paramétereit.

A napló tartalmazza:

- *a rendszerelem azonosítóját;*
- *az adatazonosítót (fájl / rekord / mező);*
- *az esemény ismertetését / a funkcióazonosítót;*
- *a felhasználó azonosítóját;*
- *az esemény időpontját;*
- *az esemény elemzéséhez szükséges adattartalmakat vagy az arra vonatkozó hivatkozásokat, illetve annak végrehajtási státuszát;*
- *valamennyi alkalmazáshibát a kivizsgálásukhoz szükséges, illetve technikailag elérhető paraméterekkel együtt.*

A rendszer a megfelelő jogosultsággal rendelkező személyek vagy szervezetek (szakmai és IT adminok, hatóság stb.) számára biztosítsa a naplózási adatok különböző szempontok szerinti lekérdezését (szervezet, szervezeten belül egy meghatározott felhasználó azonosítója vagy személyi adatai, meghatározott időpont vagy időtartam szerint stb.) a naplóadatok megtekintését, exportálhatóságát, valamint a naplóadatok időszakos archiválását.

4.6.5. Mentés, archiválás

Lehetőség szerint dedikált szerveren keresztül történjen, az archívumokat a használt technológiától függetlenül (teljes, inkrementális, differenciális mentés) fizikailag védett helyen kell tárolni. A SZEÜSZ szolgáltatás erőforrásainak tervezésekor figyelembe kell venni, hogy a mentéseknek legalább egy generációját diszk alapú tárolón célszerű tartani a gyors visszaállíthatóság érdekében.

5. Felhasznált források, hivatkozások

A hivatkozott jogszabályok mellett a következő forrásanyagok kerültek felhasználásra:

- A Közigazgatási és Igazságügyi Minisztérium ÁROP-1.2.10 projekt keretében készült vonatkozó munkaanyagai
- E-CODEX D4.2, D6.3 „Concept of Implementation", D3.3 „Documented System Requirements and Specifications", D6.2 „Standards, reusable assets and missing building blocks", D6.1 „Requirements v1"
- Európai Bizottság 1179/2011/EU végrehajtási rendelete
- Teljeskörű ügyfélazonosítás kiemelt projekt (KEK KH, EKOP 2.3.8), „Részletes Megvalósíthatósági Tanulmány "