

Deszán Kft
Informatikai Biztonsági Szabályzata (IBSZ)
Kivonat

1. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A Szabályozás célja

Deszán Kft (a továbbiakban: Társaság) Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ) célja, hogy a vonatkozó jogszabályokkal, a Társaság belső rendelkezéseivel összhangban meghatározza a Társaság informatikai rendszerei által kezelt információvagyon bizalmassága, hitelessége, sértetlensége, valamint rendelkezésre állásának biztosítása, funkcionalitása és üzembiztonsága megőrzése érdekében betartandó elveket. Az IBSZ meghatározza a vezető és a biztonságért felelős személy feladatait, valamint az információs rendszer működtetői és felhasználói számára kötelező szabályokat. Az IBSZ kiemelt célja, hogy a Társaság informatikai rendszereinek zavartalan működése biztosítva legyen.

1.2. A Szabályozás hatálya

1.2.1. Az IBSZ személyi hatálya

Az IBSZ személyi hatálya a Társaság valamennyi teljes vagy részmunkaidős, valamint szerződéses dolgozójára kiterjed. Az IBSZ hatálya kiterjed a Társaság informatikai rendszerének üzemeltetésében és karbantartásában résztvevő cégekre, vállalkozókra.

Az IBSZ hatálya kiterjed minden olyan magánszemélyre, illetve gazdasági Társaságra, aki nem informatika célú munkavégzése kapcsán bármilyen informatikai eszközzel a Társaság informatikai infrastruktúrájához csatlakozik, illetve azt – Társasági érdekből – igénybe veszi.

1.2.2. Az IBSZ tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed:

- a védelmet élvező adatok teljes körére, felmerülési és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
- a Társaság tulajdonában lévő, illetve az általa bérelt, vagy használt valamennyi informatikai berendezésre (számítógépekre, azok tartozékaira és

- továbbá tulajdonviszonytól függetlenül (tulajdonolt, bérelt, stb.) a Társaság területén (állandóan vagy ideiglenes jelleggel) telepített informatikai eszközökre, az azokkal kapcsolatos tevékenységekre.

1.2.3. Az IBSZ időbeli hatálya

Az Informatikai Biztonsági Szabályzatot évente, vagy jelentősebb infrastrukturális változás, illetve jogszabály változás esetén időközben felül kell vizsgálni és szükség esetén módosítani kell, mind Társasági, mind informatikai szakmai szempontok szerint.

1.3. Szerepkörök, tevékenységek, felelőségek

Az informatikai biztonsággal kapcsolatos feladatok szerepkörökhöz rendelve. A szerepkörök szerinti felelősök kijelölése elsősorban a munkaköri leírásokban történik. Az informatikai infrastruktúra biztonságos működtetésében, illetve az informatikai rendszerekben kezelt adatok védelmének tárgykörében a következő szerepkörök kerülnek meghatározásra.

1.3.1. A Társaság vezetője

A Társaság vezetője az ügyvezető (továbbiakban: a Társaság vezetője). Felelős az informatikai rendszerben tárolt adatok védelméért és az adatok biztonságáért. Hatáskörében jogosult a számítógépes adatvédelem és az adatbiztonság megszervezésére és ellenőrzésére.

1.3.2. Az elektronikus információs rendszerek biztonságáért felelős személy

Az elektronikus információs rendszerek biztonságáért felelős személy feladatait a műszaki igazgató (továbbiakban: IBF) látja el. Az IBF felel a Társaságnál előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért.

Az elektronikus információs rendszer biztonságáért felelős személy Társasági vezetői támogatással biztosítja az e szabályzatban meghatározott követelmények teljesülését. A Társaság valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködik.

1.3.3. Egyéb szerepkörök

1.3.3.1. Honlap tartalom kezelő

A Társaság honlapjának tartalomkezelését a Társaság egy kijelölt dolgozójának iránymutatása alapján külső szolgáltató végzi.

A honlapra kerülő adatokat, információkat különös tekintettel a jogszabály által előírt kötelezően nyilvános adatokra - változás esetén - a Társaság kijelölt dolgozója továbbítja a tartalomkezelőhöz.

1.3.4. Üzemeltetői csoport/üzemeltetők, informatikus

Ezt a feladatot a Társaságnál külső szolgáltató látja el. Feladatuk az informatikai infrastruktúra üzemeltetése, fejlesztése és biztonságos működésének elősegítése.

1.3.5. Felhasználók

A Társasági rendszerek nem Üzemeltetői csoportban lévő/nem informatikus felhasználói.

2. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK

2.1. Informatikai biztonságpolitika

A Társaság megfogalmazza és kihirdeti az informatikai biztonságpolitikát (a továbbiakban IBP), melyben meghatározza a kiberbiztonsági célokat, kifejti az alkalmazott biztonsági alapelveket és megfelelési követelményeket, valamint bemutatja a vezető beosztású tagjainak elkötelezettségét a biztonsági feladatok irányítása és támogatása iránt.

2.2. Az elektronikus információs rendszerek nyilvántartása

A Társaság az elektronikus információs rendszereiről nyilvántartást vezet. A nyilvántartást elektronikus formában vezeti, és gondoskodik azok naprakészségéről.

Minden rendszereszközt a beszerzéssel egyidejűleg fel kell venni a nyilvántartásba! A nyilvántartásból rendszereszközt kivenni csak annak selejtezésekor lehet.

2.3. Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás

Az új belépő munkatársak a belépéskori oktatás és a titoktartási nyilatkozat aláírása után kaphatnak hozzáférést a rendszerekhez. A belépő munkatárs új hozzáférési jogkörét, illetve nem új belépő munkatárs hozzáférési jogkör változtatását a Társaság vezetője határozza meg.

2.4. Személyi biztonság

A hozzáférési jogosultságot igénylő felhasználóval szembeni elvárásokat, a rá vonatkozó szabályokat, felelősségüket az adott rendszerhez kapcsolódó kötelező vagy tiltott tevékenységeket jelen dokumentum tartalmazza.

2.5. Rendszer és szolgáltatás beszerzés

2.5.1. A rendszer fejlesztési életciklusa

Az informatikai eszközök különböző beszerzési eljárás módjainak alkalmazásánál fokozottan szem előtt kell tartani, hogy a szóban forgó eszköz megfeleljen a jelen szabályzatban rögzített informatikai biztonsági követelményeknek.

3. ADATOK ÉS IT RENDSZEREK VÉDELME, BIZTONSÁGA

3.1. Fizikai védelmi intézkedések

3.1.1. Fizikai védelmi eljárásrend

A fizikai és környezeti biztonságra vonatkozó óvintézkedések a Társasági rendszereknek helyet adó létesítmények, a rendszer erőforrások és a működést biztosító alapszolgáltatások védelmével kapcsolatban fogalmazznak meg szabályokat annak érdekében, hogy a számítástechnikai szolgáltatások megszakadását, eszközök ellopását, a fizikai károkozást, az információk jogosulatlan felfedését, a rendszer sértetlenségének elvesztését.

3.2. Társasági és személyzeti szabályok

Minden, a személybiztonsággal kapcsolatos eljárás, vagy elvárás kiterjed a Társaság teljes személyi állományára, valamint minden olyan természetes személyre, aki a Társaság elektronikus információs rendszereivel kapcsolatba kerül, vagy kerülhet. Azokban az esetekben, amikor az elektronikus információs rendszereivel tényleges, vagy feltételezhető kapcsolatba kerülő személy nem a Társaság alkalmazottja, a jelen fejezet szerinti elvárásokat a tevékenység alapját képező jogviszonyt megalapozó szerződés, megállapodás, megkötés során kell, mint kötelezettséget érvényesíteni (ideértve a szabályzatok, eljárásrendek megismerésére és betartására irányuló kötelezettségvállalást, titoktartási nyilatkozatot).

3.2.1. Képzési eljárásrend

A felhasználói állományt az informatika biztonság megvalósítása érdekében munkakörüknek megfelelően képezni kell, a fejlesztői, üzemeltetői állománynak pedig folyamatosan szinten kell tartania, és fejlesztenie kell az informatikával és informatikai biztonsággal kapcsolatos ismereteit. A felhasználói személyi állományt naprakészen képezni kell új rendszerek bevezetésekor. A Társaságban alkalmazott új dolgozót soron kívül ki kell oktatni a rendszer használatáról.

3.2.2. Biztonság tudatosság képzés

A Társaság annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára.

3.2.3. Fegyelmi intézkedések

A biztonsági előírásokat megsértőkkel szemben fegyelmi eljárás indul a vonatkozó munkajogi jogszabályoknak megfelelően.

3.2.4. Eljárás a jogviszony megszűnésekor

A munkavállaló jogviszonyának megszűnése esetén a műszaki igazgató gondoskodik a kilépő információs rendszerrel vagy annak biztonságával kapcsolatos feladatainak ellátásáról a jogviszony

megszűnését megelőzően. A jogviszony megszűnésekor a műszaki igazgató gondoskodik arról, hogy a kilépő esetleges elektronikus információs rendszert, illetve abban tárolt adatokat érintő, elektronikus információbiztonsági szabályokat sértő magatartását megelőzze (hozzáférések megszüntetése, jogosultságok visszavonása).

A Társaság meghatározott ideig megtartja magának a hozzáférés lehetőségét a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és Társasági információkhoz.

3.3. Azonosítás és hitelesítés

Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a Társaság felhasználóit, a felhasználók által végzett tevékenységet.

3.3.1. Azonosítási és hitelesítési eljárásrend

A Társaságban alkalmazott informatikai rendszerekben felhasználói azonosítást és hitelesítést kell alkalmazni a jogosulatlan személyek tevékenységének megakadályozása és az elszámoltathatóság megvalósítása érdekében.

3.4. Hozzáférés védelem, jogosultság kezelés

3.4.1. Hozzáférés ellenőrzési eljárásrend

Minden, az IBSZ hatálya alá eső adatot, a központi informatikai rendszerben, a központi logikai, fizikai rendszerek védelme alatt, központi hozzáférés-védelmi és jogosultság-kezelési rendszer ellenőrzése mellett kell menedzselni az egyedi elszámoltathatóság elvének érvényre juttatásával.

3.4.2. Külső rendszerekből történő hozzáférés szabályozása

Külső cégek folyamatos üzemeltetési feladatainak ellátása érdekében (pl.: szerverek karbantartása, alkalmazások karbantartása) a cégek megbízott munkatársai állandó távoli hozzáférést kaphatnak az általuk felügyelt rendszerhez. Ezeket a hozzáféréseket a cégeknek az IBSZ betartásával, bizalmasan és a szakmai normáknak megfelelően kell kezelniük.

3.4.3. Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

A számítógépes munkahely kialakítását követően a számítógépen dolgozók azonosítására, valamint a jogosultságok meghatározására van szükség. A számítógép használatakor egyedi azonosítókat kell alkalmazni, melyek hiányában a munkaállomásra belépés nem lehetséges, így az elektronikus információs rendszeren belül semmilyen tevékenységre nincs lehetőség.

3.4.4. Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a Társaság a publikus weboldalát.

3.4.4.1. Cookie-k használata

A cookie-k (sütik) rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Az Európai Bizottság irányelvei alapján cookie-kat [kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek] csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni.

A Társaság weboldala csak felhasználó hozzájárulását nem igénylő sütiket használ. Erről a honlap látogatása során kell tájékoztatást nyújtani. Nem szükséges, hogy a sütikre vonatkozó tájékoztató teljes szövege megjelenjen, elegendő röviden összefoglalni a tájékoztatás lényegét és egy linken keresztül utalni a teljes körű tájékoztató elérhetőségére.

3.5. Viselkedési szabályok az interneten

A Társaság e-mail és Internet használati jogokkal rendelkező dolgozói a munkájukkal kapcsolatban használhatják a Társaság által biztosított Internet szolgáltatást.

A Társaság vezetőjének joga van az Internet-hozzáférés tartalmi, időbeli, sávszélességbeli és szolgáltatásbeli korlátozásához, amennyiben ez az Internet Társasági célú használatának biztosításához szükségessé válik. A korlátozásról a felhasználókat előzetesen tájékoztatni kell.

3.5.1. Elektronikus levelezés (e-mail)

Az e-mail szolgáltatás a Társaság által a felhasználók részére a Társasági elektronikus levelezés céljaira biztosított eszköz. Az e-mail rendszer, valamint a rendszerben előállított, elküldött és megkapott levél is a Társaság felügyelete alá tartozik.

4. AZ INFORMATIKAI RENDSZEREK ÜZEMELTETÉSE

4.1. Általános rendelkezések

Az Üzemeltetői csoport/informatikus feladata a felhasználók informatikai támogatása, a szolgáltatások folyamatos, Társasági időben való rendelkezésre állásának biztosítása, a felmerülő biztonsági problémák azonosítása, azok megbízható kezelése és a biztonságért felelős személy tájékoztatása a felmerült problémákról, észlelt jelenségekről.

Az informatikai eszközöket rendeltetésszerűen kell használni: a számítógépen és perifériáin papírokat és egyéb tárgyakat tárolni nem lehet, a szellőző nyílásokat szabadon kell hagyni, a billentyűzetet védeni kell a szennyeződésektől, a számítógép közelében enni-inni, dohányozni nem szabad!

4.2. Konfigurációkezelés

4.2.1. Alapkonfiguráció

A Társaság:

- az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa;
- meghatározza a tiltott vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

4.3. Szoftverhasználat korlátozásai

A Társaság bármely informatikai rendszerére csak az Üzemeltetői csoport munkatársai/informatikus telepíthetnek szoftvert, *a felhasználónak szoftvertelepítésre és bizonyos beállítások módosítására nincs sem joga, sem lehetősége.* A Társaság informatikai eszközeire TILOS illegális és/vagy nem jogtiszt szoftvert telepíteni! A Társaság informatikai infrastruktúrájában a feladatok végrehajtására kizárólag a Társaság által megvásárolt licencű kereskedelmi szoftver termékeket és/vagy szabad szoftvereket lehet alkalmazni. Minden illegális, vagy nem a munkavégzést szolgáló szoftvert, adatot törölni kell a rendszerből. Ezt a műveletet a felhasználó tudtával és az Üzemeltetői csoportvezető/informatikus engedélyével az Üzemeltetői csoport munkatársa/informatikus végzi el.

Illegális szoftverek használata esetén a felhasználóval szemben felelősségének megállapítása érdekében fegyelmi, kártérítési, illetve egyéb eljárás indulhat.

A telepítést megelőzően a Társaságban vírusvédelmi célokra üzembe állított eszközzel meg kell vizsgálni a szoftver esetleges vírusfertőzöttségét. Amennyiben technikailag/technológiailag lehetséges, úgy az új szoftvercsomagról biztonsági másolatot kell készíteni. Az installálást csak a munkapéldányról szabad végezni. Az eredeti példányt biztonságos helyen kell tárolni.

A Társaság infrastruktúrájában található eszközökre idegen program, adat másolása tilos!

4.3.1. Felhasználó által telepíthető szoftverek

A felhasználók az informatikai eszközöket Társasági munkavégzés céljára kapják. A felhasználók jogosultsága a belső hálózaton csak a rendszergazda által telepített egységes irodai alkalmazások és szolgáltatások használatára, illetve a munkájukhoz szükséges alkalmazói programok futtatására terjed ki. A Társaság informatikai infrastruktúráját magán célú használatra igénybe venni TILOS!

Ettől eltérni csak a Társaság vezetője vagy az Információbiztonsági Felelős (IBF) engedélyével, akkor is kizárólag mobil eszközök esetében szabad (notebook, tablet, mobiltelefon, mobil adathordozók).

4.4. Adathordozók védelme

4.4.1. Adathordozók védelmére vonatkozó eljárásrend

A Társaság által használt hordozható külső adattárolókat (flash diskek, USB pendrive-ok, memóriakártyák, hordozható hdd-k és ssd-k) egyedi azonosítóval kell ellátni, kivételt képeznek ez alól az optikai adathordozók (CD, DVD) és a floppy lemezek, amely tárolók csak számszerűen kerülnek

nyilvántartásba. Az egyedi azonosítóval ellátott hordozható adathordozók pontos helyéről naprakész adatbázist kell vezetni.

4.4.2. Adathordozók használata, hozzáférés az adathordozókhoz

A Társasági informatikai rendszerekben kezelt adatok, dokumentumok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell, ezért a Társaság nyilvántartást vezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek köréről, valamint jogosítványuk tartalmáról. A nyilvántartást rendszeres időközönként felülvizsgálja, aktualizálja.

Minden munkatársnak kötelessége az adattárolók rendeltetésszerű használata. A Társaság adathordozói csak a munkavégzéshez szükséges adatok és szoftverek tárolására hivatottak.

4.4.3. Adathordozók újrahaználása, leselejtezése, megsemmisítése

Az adathordozók biztonságához szorosan kapcsolódik az, hogy adathordozók újrahaználása, illetve selejtezése után is biztosítani kell a védendő adatok bizalmasságát.

Amennyiben az adathordozó oly mértékben sérült vagy elhasználódott, hogy a további használata lehetetlen vagy célszerűtlen, úgy azt selejtezni, majd megsemmisíteni kell.

A selejtezési eljárás folyamán az adathordozókon olyan eljárást kell végrehajtani, amelyek megakadályozzák azt, hogy a későbbiekben ezekről az eszközökről adatokat lehessen visszanyerni.

4.5. Felkészülés a rendkívüli helyzetekre, katasztrófákra

4.5.1. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

Kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

A kidolgozott stratégiákban felelősöket kell kijelölni.

4.6. Az elektronikus információs rendszer mentései

A Társasági informatikai rendszerekben kezelt adatok, dokumentumok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását biztosítani kell.

A biztonsági mentések gyakoriságának összhangban kell állnia a mentett adatok, illetve programok elvesztésük, sérülésük kockázatával és hatásával, valamint a Társaság ügyintézési ciklusával.

A mentési rendszert a technológiai és gazdasági lehetőségek figyelembevételével a lehető legnagyobb mértékben automatizálni kell, hogy minimalizálni lehessen az emberi tényezőtől adódó hibák előfordulásának valószínűségét.

A mentéseken kívül meghatározott időközönként archiválást kell végezni a központi rendszerekben tárolt felhasználói adatokról.

4.7. Az elektronikus információs rendszer helyreállítása és újraindítása

A Társaság Üzemeltetői csoportja/informatikusa gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

4.8. Karbantartás

4.8.1. Rendszeres karbantartás

A Társaság:

- a karbantartásokat és javításokat ütemezetten hajtja végre;
- jóváhagyja és ellenőrzi az összes karbantartási tevékenységet;

5. RENDSZER ÉS INFORMÁCIÓ SÉRTETLENSÉG

Ezeket a rendelkezéseket egy adott elektronikus információs rendszer tekintetében abban az esetben kell alkalmazni, ha az adott elektronikus információs rendszert a Társaság üzemelteti. Üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell az alábbiakat érvényesíteni, és azokat a szolgáltatónak kell biztosítania.

5.1. Felügyelet

A biztonsági események olyan események, melyek eltérnek a megszokott ügymenettől, zavarokat okozhatnak és fenyegethetik az információk, illetve az információ feldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

Az információbiztonsági incidensek olyan biztonsági események, melyek ténylegesen fenyegetik az információk, illetve az információ feldolgozó eszközök bizalmasságát, sértetlenségét és rendelkezésre állását.

5.1.1. Felügyeleti eszközök

Az elektronikus információs rendszer felügyeleti információit az Üzemeltetői csoport/informatikus rendszeresen elemzi, igény esetén jelentést készít azokról. Fokozott kockázatra utaló jelek észlelése esetén javaslatokkal él.

5.2. Incidensek kezelése

Az incidensek kezelése során a Társaság vezetője és az IBF döntenek a szükséges lépésekről.

- A biztonsági incidensek érintett rendszerelemeit, a minősítést követően lokalizálni kell és megakadályozni az esetleges tovább terjedést.
- Be kell gyűjteni az összes adatot és bizonyítékot.
- Gondoskodni kell a károk enyhítéséről.

5.3. Naplózás

A Társaság informatikai rendszereinek tervezésekor rögzített naplózási szabályokat kell alkalmazni.

5.3.1. Naplózható események

A Társaság:

- meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;
- megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

5.3.2. Naplóinformációk védelme

Az elektronikus információs rendszert úgy kell felépíteni, hogy az megvédi a naplóinformációt és a napló-kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

5.4.3 Napló tárhelykapacitás

A Társaság a naplózásra elegendő méretű tárhelykapacitást biztosít.

5.4 Kártékony kódok elleni védelem

A lehetséges informatikai biztonsági fenyegetések közül igen jelentős kockázatot jelentenek a rosszindulatú programok és kódok, a levélszemetek (spam), és a káros Internet tartalmak. A felsorolt negatív elemek ellen számos technológiai eszközzel lehet védekezni, ilyenek a biztonságos átjárók, tűzfalak, vírusvédelmi eszközök, levélszemét szűrő szoftverek, IDS-ek és IPS-ek.

A hálózati határvédelem elsősorban a megelőzésre, másodsorban az elhárításra szolgál. A vírustámadások nagy része az internet, és a levelező rendszerek közreműködésével valósul meg.

A Társaság számítógépes hálózatát, szervereit és munkaállomásait folyamatosan, illetve az adott számítástechnikai eszközt a felhasználó jelzése alapján vírusvédelmi szempontból figyelni kell. A vírusfertőzés ellenőrzéséről és annak eredményéről nyilvántartást kell vezetni (a legtöbb vírusvédelmi rendszer ezt magától megteszi).

A preventív vírusvédelmet, a tartalom és spam szűrést és a hálózati határvédelmet hardver és eszközök és szoftver megoldások biztosítják. Ezek kiszűrik a vírusos üzeneteket és a kéretlen leveleket, valamint *letiltják meghatározott weblapok megnyitását.*

5.5 Hibajavítás, biztonsági frissítések

A Társaság által használt szoftverek hibáinak napvilágra kerülése esetén számítani lehet arra, hogy az ártó szándékú támadók ezeket a biztonsági réseket kihasználva próbálnak az információs rendszerébe behatolni, ezért elengedhetetlen, hogy a szoftver gyártója által készített javítások (frissítések) a lehető leghamarabb a telepítésre kerüljenek.

6 RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM

6.4 Rendszer- és kommunikációvédelmi eljárásrend

6.4.1 Túlterhelés – szolgáltatás megtagadás alapú támadás – elleni védelem

Az elektronikus információs rendszer véd a túlterheléses (ügynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

6.5 Határok védelme

Az elektronikus információs rendszer felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt. A zónák közötti kommunikáció csak szabályozott formában, határvédelmi rendszer beiktatásával biztosítható.

A hálózati határvédelem eszközeinek működését folyamatosan ellenőrizni kell, annak rendszeres frissítéséről kiemelt figyelemmel kell gondoskodni!

Deszán Kereskedelmi és Szolgáltató Kft

Kelt: Martfű, 2018. év május hó 25. nap