JAVASLAT

Az elektronikus hírközlésről szóló törvény (130/22. és 18/23. sz. UL RS – ZDU-1O) 116. cikkének (6) bekezdése értelmében a Szlovén Köztársaság Hírközlési Hálózati és Szolgáltatási Ügynöksége, figyelembe véve a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról szóló, 2015. szeptember 9-i (EU) 2015/1535 európai parlamenti és tanácsi irányelv (HL L 241., 2015.9.17., 1. o.) szerinti tájékoztatási eljárást, a következőt bocsátja ki:

ÁLTALÁNOS JOGI AKTUS
a kiegészítő biztonsági követelményekről és korlátozásokról

1. cikk
(Az általános jogi aktus tartalma)

A jelen általános jogi aktus a következőkről rendelkezik:

1. a következők által követendő iránymutatások: azon mobil hírközlő hálózatok üzemeltetői (a továbbiakban: üzemeltetők), amelyek ezeket a hálózatokat olyan kritikus fontosságú szervezetek számára biztosítják, amelyek a kritikus infrastruktúra szabályozásának más területein a kritikus infrastruktúrák területét szabályozó jogszabályokban meghatározottak szerint kritikus infrastruktúrákat üzemeltetnek (a továbbiakban: kritikusinfrastruktúra-üzemeltetők); az információbiztonságot szabályozó törvény által meghatározott alapvető szolgáltatásokat nyújtó szolgáltatók (a továbbiakban: alapvető szolgáltatások szolgáltatói); az információbiztonságot szabályozó törvény által meghatározott államigazgatási szervek (a továbbiakban: államigazgatási szervek) vagy az ország biztonsági rendszerét alkotó kulcsfontosságú elemek birtokosai; és
2. a hálózat és az elektronikus hírközlésről szóló törvény (130/22. és 18/23. sz. UL RS – ZDU-1O) (a továbbiakban: a törvény) 116. cikkének (6) bekezdésében említett funkciókkal rendelkező kapcsolódó információs rendszerek kritikus elemeinek birtokosai; a mellékletben foglaltak szerint, amely ezen általános jogi aktus szerves részét képezi, és amelyet az információbiztonságért felelős szervvel együttműködésben készítenek el.

2. cikk
(Fogalommeghatározások)

(1) A jelen általános jogi aktusban használt kifejezések a következőket jelentik:

1. ellátási lánc: az üzemeltető hálózatában vagy az üzemeltető számára ilyen szolgáltatásokat nyújtó felhőszolgáltatónál telepített kritikus hálózati elemek alkotóelemeinek a tervezésében, előállításában, tárolásában, forgalmazásában és szállításában, illetve telepítésében és karbantartásában részt vevő folyamatok, személyek, szervezet és elosztás teljes rendszere.

2. A hálózat kritikus elemei az ezen általános jogi aktus mellékletében felsorolt, az üzemeltetőnél vagy a felhőszolgáltatónál fizikai, szoftveres vagy virtualizált formában

működő hálózati elemek, funkciók, szolgáltatások és támogató információs rendszerek.

3. kritikus fontosságú szervezetek: a kritikus infrastruktúrákra vonatkozó szabályozás egyéb területein működő, a kritikus infrastruktúrák területét szabályozó jogszabályokkal összhangban meghatározott kritikusinfrastruktúra-üzemeltetők, az információbiztonságot szabályozó törvény értelmében meghatározott alapvető szolgáltatások szolgáltatói, az információbiztonságot szabályozó törvény értelmében meghatározott államigazgatási szervek és az ország biztonsági rendszerét alkotó kulcsfontosságú elemek birtokosai.

(2) A jelen általános jogi aktusban használt egyéb kifejezések jelentése megegyezik a törvényben, valamint a hálózatok, szolgáltatások és adatok biztonságáról szóló általános jogi aktusban meghatározottakkal.

3. cikk
(Általános iránymutatások)

(1) A kritikus hálózati elemek alkotóelemeinek ellátási láncában részt vevő üzemeltetőknek és az ezen alkotóelemekre vonatkozó harmadik szintű támogatási szolgáltatásoknak ezen alkotóelemek teljes életciklusa során legalább a következő iránymutatásokat kell követniük:

1. az egyes gyártók vagy beszállítók, valamint harmadik szintű támogató szolgáltatók esetében a velük fennálló kapcsolatok és megállapodások miatt, a köz- vagy magánjog hatálya alá tartozó, természetes vagy jogi személynek minősülő harmadik felek (a továbbiakban: harmadik felek) általi beszállítás és lehetséges hatások, a más gyártók berendezéseivel való kompatibilitás, a termékminőség és -biztonság, valamint az üzemeltető és a kritikus fontosságú szervezetek szolgáltatásainak működésére gyakorolt negatív hatások tekintetében kockázatértékelést kell végezniük;
2. hogy a biztonság beépített és már a tervezés során megvalósult, és hogy a szerződések előírják az észlelt sebezhetőségek kiküszöbölésének határidejét;
3. hogy a kulcsfontosságú biztonsági jellemzők (rendelkezésre állás, titkosság, sértetlenség és hitelesség) használatuk teljes élettartama során biztosítottak legyenek;
4. hogy a biztonság és szünetmentes tápellátásuk garantált, és igazolt, hogy a nemzetközileg elismert szabványokkal (3GPP) és az európai műszaki szabványokkal (ETSI) összhangban magas szintű biztonsági jellemzőket támogat;
5. hogy az e bekezdés 2–4. pontjában említett iránymutatások a gyártóval vagy a beszállítóval kötött szerződéses dokumentációban ellenőrizhetők;
6. minden egyes gyártó vagy beszállító esetében értékelik és figyelembe veszik a berendezések gyártásához és használatához szükséges kulcsfontosságú technológiák használatára vonatkozó jogokkal összefüggő kockázatokat, valamint a berendezések, pótalkatrészek vagy harmadik szintű támogató szolgáltatások szállításával összefüggő kockázatokat;
7. hogy a felhasznált alkotóelemeknek nincsenek megoldatlan ismert kritikus vagy aktívan kihasznált sebezhetőségeik;
8. egyetlen gyártó vagy beszállító elkerülése, amennyiben ez műszakilag megvalósítható és gazdaságilag fenntartható, a függőség csökkentése és az ellenálló képesség növelése céljából a kritikus alkotóelemek sebezhetősége, a

katasztrofális hálózati meghibásodások vagy a kritikus fontosságú szervezetek hálózatainak és szolgáltatásainak biztonságát érintő, a köz- vagy magánjog hatálya alá tartozó, természetes vagy jogi személyeknek minősülő harmadik felek általi fenyegetés esetén.

(2) Az információs és kommunikációs berendezések, rendszerek és szolgáltatások beszállításakor az üzemeltetőknek teljes mértékben meg kell felelniük az Európai Unió Kiberbiztonsági Ügynöksége (a továbbiakban: ENISA) iránymutatásainak és az Európai Uniónak a biztonságos IKT-termékek és -szolgáltatások beszerzése során alkalmazandó alapvető biztonsági követelményekre vonatkozó érvényes előírásainak. Az Ügynökség honlapján közzéteszi és naprakészen tartja az ENISA fent említett területre vonatkozó aktuális dokumentumaira és uniós szabályozásaira mutató linkeket.

(3) A kritikus hálózati elemek alkotóelemeinek szállításakor vagy felhőalapú szolgáltatások igénybevételekor azoktól a gyártóktól vagy beszállítóktól származó alkotóelemeket, illetve azoktól a felhőszolgáltatóktól származó szolgáltatásokat kell előnyben részesíteni, amelyeket akkreditált és szükséges esetben az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendelet (a továbbiakban: rendelet) 60. cikkének (3) bekezdése alapján a rendelet 52. cikkében meghatározott megbízhatósági szintű európai kiberbiztonsági tanúsítványok kiállítására felhatalmazott megfelelőségértékelő szervezetek tanúsítottak.

(4) Az előző bekezdés alkalmazásában az üzemeltetőnek ellenőriznie kell egy, az ENISA által a rendelet 55. cikkével összhangban létrehozott külön weboldalt, amelynek célja, hogy tájékoztassa a nyilvánosságot az európai kiberbiztonsági tanúsítási rendszerekről, az európai kiberbiztonsági tanúsítványokról és az EU-megfelelőségi nyilatkozatokról, beleértve a már nem érvényes vagy visszavont és lejárt európai kiberbiztonsági tanúsítványokra és EU-megfelelőségi nyilatkozatokra vonatkozó információkat, valamint a kiberbiztonsági információkra mutató linkeket tartalmazó adattárat.

4. cikk
(Kockázatértékelés)

(1) A hálózat kritikus elemei közé tartozó alkotóelemek gyártójával vagy beszállítójával és harmadik szintű szolgáltatójával összefüggő kockázat meghatározásakor az üzemeltető a következő kockázati szempontokat veszi figyelembe, amelyeket értékel.

(2) Az előző bekezdésben említett értékelés során az üzemeltetőnek legalább a következőket kell értékelnie és figyelembe vennie:

1. általános minőség (beleértve a biztonsági szempontokat is) és megbízhatóság;
2. a nyílt szabványok és interfészek használatának szintje, amelyek megakadályozzák az adott gyártó vagy beszállító termékeitől való függőséget és az azokkal kapcsolatos kényszerhelyzetet;
3. az elismert nemzetközi és európai műszaki szabványoknak (3GPP, ETSI) és az Európai Unió előírásainak és az alapértelmezett biztonsági beállításoknak való megfelelés a szakmai ajánlásokkal összhangban (GSMA Szövetség);
4. a harmadik felek berendezéseivel és hálózati funkcióival való kompatibilitás szintje;

5. frissítések és testreszabások biztosításának képessége;
6. sebezhetőségkezelési folyamat, közzétételük, valamint a frissítések és javítások naprakészsége;
7. dokumentáció elérhetősége és átláthatósága a következőkre vonatkozóan:
   - kulcsfontosságú funkciók és információk az alkotóelem biztonsági és egyéb jellemzőiről, valamint a lehetséges beállításokról, és
   - használt szoftver, beleértve a nyílt forráskódot (Anyagjegyzék – SBOM);
8. a harmadik szintű támogató szolgáltatásoktól való függés szintje a berendezések kezelése és karbantartása során, ha az üzemeltető nem egyedül, az alkalmazottai közreműködésével végzi ezeket a szolgáltatásokat;
9. a berendezés vagy harmadik szintű támogatási szolgáltatást nyújtó szervezet megfelelőségének előzetes értékelése az Európai Unióban az európai kiberbiztonsági tanúsítási rendszereknek megfelelően akkreditált szervek által, és az akkreditált szervek közzététele az Európai Unió Hivatalos Lapjában.

(3) Az üzemeltetőnek minden egyes kiválasztott gyártóra vagy beszállítóra vagy harmadik szintű szolgáltatóra vonatkozóan dokumentálnia kell az e cikk (2) és (3) bekezdésében említett kockázati tényezőket és a kockázatértékelés eredményeit, és ezt rendszeresen frissítenie kell.

5. cikk
(A kritikus hálózati elemek működésére vonatkozó általános iránymutatások)

(1) A kritikus hálózati elemek alkotóelemei, azok működési és alapértelmezett beállításai nem tartalmazhatnak olyan műszaki jellemzőket, amelyek – többek között szabotázs, kémkedés, szellemi tulajdon ellopása vagy terrorizmus miatt – negatívan befolyásolhatják a kritikus fontosságú szervezetek biztonságát vagy működését.

(2) A kritikus hálózati elemek általában a Szlovén Köztársaságban, vagy – az összes biztonsági kockázatot figyelembe véve, és magas szintű biztonsági intézkedéseket megvalósítva –, és ha ezt a vonatkozó rendeletek másként nem határozzák meg, az Európai Unióban találhatók. A tervezett áthelyezésükről az üzemeltető a Szlovén Köztársaság Hírközlési Hálózati és Szolgáltatási Ügynökséget (a továbbiakban: az Ügynökség) és az információbiztonságért felelős szervet az Európai Unión kívüli áthelyezés előtt legalább 30 nappal köteles tájékoztatni.

(3) A hálózat kritikus elemeinek harmadik szintű támogatási szolgáltatásait általában a Szlovén Köztársaságban, vagy – az összes biztonsági kockázatot figyelembe véve és magas szintű biztonsági intézkedéseket megvalósítva –, és ha ezt a vonatkozó rendeletek másként nem határozzák meg, az Európai Unióban végzik. A harmadik szintű támogató szolgáltatásainak tervezett áthelyezéséről az üzemeltető az Ügynökséget és az információbiztonságért felelős szervet az Európai Unió tagállamain kívülre történő áthelyezés előtt legalább 30 nappal köteles értesíteni.

(4) A harmadik szintű támogató szolgáltatások megvalósítása nem veszélyeztetheti a kritikus fontosságú szervezetek szolgáltatásainak biztonságát vagy működését, illetve a nemzetbiztonságot.

(5) Az üzemeltető létrehozza és rendszeresen végrehajtja a kritikus hálózati elemek azonosításának folyamatát. Ezt évente legalább egyszer, vagy a kritikus hálózati elemek alkotóelemeinek beszerzésekor kell elvégezni.

(6) Ha egy adott alkotóelem csak részben képvisel kritikus hálózati elemet, azt egy kritikus hálózati elem részének kell tekinteni.

(7) Az üzemeltető naprakész jegyzéket vezet a kritikus hálózati elemek valamennyi alkotóeleméről, azok funkcióiról, helyéről, rendszergazdáiról és kezelőiről, harmadik szintű támogató szolgáltatóiról és gyártóiról vagy beszállítóiról. Kérésre a jegyzéket az Ügynökség és az információbiztonságért felelős szerv rendelkezésére kell bocsátani.

6. cikk
(A kritikus hálózati elemek alkotóelemeinek szállítására vonatkozó biztonsági intézkedések)

(1) Az üzemeltetőnek ismernie kell a teljes ellátási láncot és az ahhoz kapcsolódó kockázatokat, ideértve a kritikus hálózati elemek egyes alkotóelemeinek alvállalkozóit is, beleértve a titkosítási kulcsokat, az UICC/eUICC-t és más olyan biztonsági elemeket is, amelyek helytelen használata veszélyeztetheti a kritikus fontosságú szervezetek biztonságát.

(2) Az üzemeltető biztosítja, hogy az üzemeltető és a kritikus hálózati elemek alkotóelemeinek gyártói vagy beszállítói vagy harmadik szintű támogató szolgáltatói közötti biztonsági követelményekről szerződésben állapodjanak meg és dokumentálják azokat, és előírják a gyártók vagy beszállítók számára, hogy a szerződésben foglalt biztonsági intézkedéseket az ellátási lánc egészében betartsák.

(3) A sebezhetőségek rosszindulatú kihasználásának időbeni megakadályozása érdekében az üzemeltetőnek biztosítania kell, hogy a kritikus hálózati elem alkotóelemeinek gyártója vagy szállítója szerződésben vállalja, hogy haladéktalanul tájékoztatja az üzemeltetőt a feltárt sebezhetőségről és a kockázatok csökkentésére irányuló intézkedésekről, és tanácsot ad azokról a védelmi vagy helyreállító intézkedésekről, amelyeket az üzemeltető a fenyegetésre válaszul megtehet.

(4) Az üzemeltetőnek évente legalább egyszer ellenőriznie kell a kritikus hálózati elemek hozzáférési jogainak helytállóságát, vagy a szervezetben vagy a harmadik szintű támogató szolgáltatók oldalán bekövetkezett változásoknak megfelelően haladéktalanul frissítenie kell azokat.

(5) Amennyiben ez műszakilag megvalósítható és gazdaságilag fenntartható, az üzemeltetőnek meg kell akadályoznia az egyéni szolgáltatótól vagy harmadik szintű szolgáltatótól való függését (azaz a „vendor lock-in”-t), azzal a céllal, hogy csökkentse a függőséget és növelje az ellenálló képességet a kritikus elemek sebezhetősége terén, többek között azáltal, hogy elkerüli az egyes gyártókkal vagy beszállítókkal vagy harmadik szintű támogató szolgáltatásokat nyújtó szolgáltatókkal kötött hosszú távú szerződéseket, vagy lehetőséget biztosít e szerződések módosítására a kritikus fontosságú szervezetek számára nyújtott szolgáltatások zavarainak a lehető legalacsonyabb szintre történő csökkentése céljából.

7. cikk
(A gyártókkal, beszállítókkal vagy harmadik szintű támogató szolgáltatókkal kötött szerződések feltételei)

A magas szintű biztonság szavatolása érdekében a gyártókkal, beszállítókkal vagy harmadik szintű támogató szolgáltatókkal kötött új szerződések feltételei közé az üzemeltetőnek legalább a következőket kell belefoglalnia:

1. a gyártó vagy a beszállító nyilatkozata arról, hogy az alkotóelemnek vagy alapértelmezett beállításainak nincsenek dokumentálatlan „hátsó ajtói”, illetve nincs negatív hatása a kritikus fontosságú szervezetek működésére;
2. a gyártó, a szolgáltató vagy a harmadik szintű szolgáltató azon kötelezettségvállalása, hogy megvédi azokat az adatokat, amelyekről a szolgáltatásnyújtás során vagy a hozzáférési szolgáltatás nyújtásával összefüggésben a hozzájuk való hozzáférés során tudomást szerzett;
3. a gyártó vagy a szállító vagy a harmadik szintű szolgáltató kötelezettségvállalása, hogy haladéktalanul tájékoztatja az üzemeltetőt a kommunikációs adatok vagy forgalmi adatok védelmének olyan megsértése esetén, amely érinti vagy érintheti az üzemeltetőt vagy a jelen általános jogi aktus 1. cikke 1. pontjában említett kritikus fontosságú szervezeteket;
4. a gyártó, a szállító vagy a harmadik szintű szolgáltató kötelezettségvállalása, hogy haladéktalanul értesíti az üzemeltetőt minden olyan biztonsági eseményről és sebezhetőségről, amely hatással lehet az üzemeltető hálózatának, kapcsolódó szolgáltatásainak vagy adatainak biztonságára;
5. a gyártó vagy a szállító vagy a harmadik szintű szolgáltató kötelezettségvállalása, hogy betartja az üzemeltető által meghatározott biztonsági előírásokat és szabályokat, és megteszi a megfelelő biztonsági intézkedéseket az információs rendszerek és hálózatok, valamint az üzemeltető vagy kritikus fontosságú szervezet adatainak biztonsága érdekében;
6. az üzemeltető lehetősége a harmadik szintű támogató szolgáltató által az üzemeltető hálózatához és adataihoz való hozzáféréskor használt környezetek, eljárások, biztonsági intézkedések és eszközök bármely időpontban megvalósított ellenőrzésére;
7. a gyártó, a szállító vagy a harmadik szintű támogató szolgáltató felelőssége olyan károkért, amelyeket a kritikus hálózati elemek alkotóelemeinek azonosított sebezhetősége vagy helytelen használata, azok alapértelmezett beállítása által vagy harmadik szintű támogató szolgáltatások nyújtása során okoztak, amelyek a gyártó, a szállító vagy a harmadik szintű támogató szolgáltató gondatlansága vagy szándékos cselekedete miatt következtek be;
8. a gyártó vagy szállító vagy harmadik szintű támogató szolgáltató személyzetének az adatbiztonsági és információs rendszerekre és hálózatokra irányuló rendszeres képzésére vonatkozó kötelezettség.

8. cikk
(A kritikus hálózati elemekhez való hozzáférésre és azok használatára vonatkozó szabályok)

(1) A kritikus hálózati elemek alkotóelemeihez, azok beállításaihoz és az üzemeltető azokban tárolt, feldolgozott vagy módosított adataihoz való fizikai vagy logikai hozzáféréskor az üzemeltetőnek biztosítania kell, hogy:

1. a hozzáférés szigorúan azokra a személyekre korlátozódik, akiket erre azt megelőzően felhatalmaztak;
2. az üzemeltető ellenőrzi a kritikus hálózati elemeken a helyszínen vagy távoli hozzáférésen keresztül végzett valamennyi munkát;
3. azok a felhasználók, akikhez a kritikus hálózati elemek egyes alkotóelemeihez, azok beállításaihoz vagy az ott tárolt vagy feldolgozott adatokhoz való hozzáféréshez a legmagasabb jogosultságok vannak hozzárendelve, többtényezős hitelesítésen esnek át;
4. a hozzáférési jogosultsággal rendelkező valamennyi személynek külön felhasználói fiókja és jelszava van;
5. kizárólag olyan jelszavakat használnak, amelyeket rendszeresen vagy visszaélés észlelésekor azonnal módosítanak, és amelyek legalább 15 karakterből állnak, valamint nagy- és kisbetűket, számokat és speciális karaktereket tartalmaznak, amennyiben ezt a szoftver lehetővé teszi;
6. a hozzáférésre lehetőség szerint a zéró tolerancia vagy bizalom koncepcióját alkalmazzák;
7. a felhatalmazott felhasználó és az egyes alkotóelemek közötti kommunikációs kapcsolat biztonságát olyan titkosítással védik, amely az információbiztonság legfejlettebb technológiáin és legjobb ipari bevált gyakorlatain alapszik, vagy amelyet az információbiztonság területén működő intézmények ajánlottak;
8. a hozzáféréseket és a hozzáférési kísérleteket kitörölhetetlenül rögzítik, ezeket legalább 6 hónapig megőrzik, beleértve a biztonsági másolatot is, de ez lehet egy hosszabb időszak is, ha a kockázatkezelés elemzése és a kockázatok elfogadható szintjének értékelése azt mutatja, hogy a nyilvántartások hosszabb idejű megőrzésével a kockázatok megfelelően kezelhetők;
9. az alkotóelemekre vonatkozó összes szoftverbeavatkozást rögzítik és nyomon követik, lehetőség szerint a konfigurációmódosításokat is beleértve. A nyilvántartásokat, beleértve ezen adatok biztonsági másolatát is, az előző pontban megjelölt ideig kell megőrizni;
10. az egyes alkotóelemekhez és az azokon tárolt vagy feldolgozott adatokhoz való hozzáférés időben korlátozott és csak a szükséges munka időtartamára nyitott.

(2) Abban az esetben, ha egy harmadik szintű támogató szolgáltató személyzete vagy alkalmazottai férnek hozzá a kritikus hálózati elemek egyes alkotóelemeihez:

1. csak biztonságos közbenső munkaállomást („jump server”) használhatnak, amelyet rendszeres biztonsági ellenőrzésnek kell alávetni;
2. egy dedikált munkaállomásra csak feltétlenül szükséges eszközöket, alkotóelemeket és aktív szolgáltatásokat telepíthetnek a hálózat egyéb erőforrásaihoz való hozzáféréshez, amelyek feltétlenül szükségesek, és amelyeket a legújabb biztonsági javításokkal kell frissíteni;
3. egy dedikált munkaállomáson biztonságos kriptográfiai műveleteket és kulcsokat használnak, amely munkaállomásnak az üzemeltető hálózatában kell lennie, és az üzemeltető kizárólagos ellenőrzése alatt kell állnia;

4. minden hozzáférést az üzemeltető engedélyez, és manuálisan csak a hozzáférés időtartamára aktivál;
5. az üzemeltető fizikailag ellenőriz és rögzít minden hozzáférést és tevékenységet;
6. kéttényezős hitelesítést és legalább 15 karakter hosszúságú, nagy- és kisbetűket, számokat és speciális karaktereket tartalmazó jelszavakat kell használni, amelyeket az értékelt kockázatok alapján meg kell változtatni.

(3) Mielőtt az üzemeltető a kritikus hálózati elemek vagy azok egyes alkotóelemei kezelésével, karbantartásával vagy frissítésével kapcsolatos szolgáltatást harmadik félnek átadná, ellenőriznie és biztosítania kell, hogy az adott fél az üzemeltető saját mechanizmusaihoz és folyamataihoz képest legalább ugyanolyan vagy jobb biztonsági mechanizmusokkal és biztonságirányítási eljárásokkal rendelkezik. Az említett átadás szándékáról haladéktalanul tájékoztatja az érintett kritikus fontosságú szervezetet, az Ügynökséget és az információbiztonságért felelős szervezetet.

(4) Az üzemeltetőnek a szolgáltatásnyújtás megkezdése előtt, majd azt követően legalább évente egyszer ellenőriznie kell a biztonsági folyamatok aktuális állapotát. Az üzemeltető a harmadik fél általi támogató szolgáltatások nyújtására vonatkozó belső felülvizsgálatokról és ellenőrzésekről nyilvántartást vezet, és azt a szolgáltatások nyújtásának időtartamára és a befejezésüket követő egy évig, de legfeljebb öt évig megőrzi.

ÁTMENETI ÉS ZÁRÓ RENDELKEZÉS

9. cikk
(Átmeneti rendelkezések)

(1) Az üzemeltető ezen általános jogi aktus hatálybalépésétől számított 30 napon belül értesíti az Ügynökséget és az információbiztonságért felelős szervet a kritikus hálózati elemek meglévő helyszíneiről.

(2) Az üzemeltető ezen általános jogi aktus hatálybalépésétől számított 30 napon belül értesíti az Ügynökséget és az információbiztonságért felelős szervet a kritikus hálózati elemekre vonatkozó harmadik szintű támogató szolgáltatások meglévő helyszíneiről.

(3) Az Ügynökség az ezen általános jogi aktus 3. cikkének (2) bekezdésében említett dokumentumokat első alkalommal a jogi aktus hatálybalépésének napján teszi közzé.

10. cikk
(Hatálybalépés)

Ez az általános jogi aktus a Szlovén Köztársaság Hivatalos Közlönyében való kihirdetését követő harmincadik napon lép hatályba, és az üzemeltetők esetében a törvény 312. cikkének (2) és (3) bekezdésében meghatározott határidők lejártáig megengedett a berendezések használata és a harmadik szintű támogató szolgáltatások nyújtásának folytatása.

Sz. _____ mag. Marko Mišmaš

Ljubljana, (dátum) igazgató

EVA 2023-3150-0034

JAVASLAT

Melléklet

A kritikus hálózati elemek és a kapcsolódó információs rendszerek jegyzéke:

Kritikus hálózati elemek	**A hálózati és információs rendszerek funkciói**
Előfizető-kezelés és titkosítási mechanizmusok	- Munkamenetek kezelése (hang és adatok), - a felhasználók és berendezések hálózattal való hitelesítése, - az előfizetők és hálózati alkotóelemek (UICC/eUICC, digitális tanúsítványok/HSM) engedélyezéséhez szükséges kulcsok kezelése és tárolása, - a biztonságos hitelesítést, a kommunikáció integritásának védelmét (titkosítás) és a felhasználói kulcsok, hálózati és menedzsment alkotóelemek tárolását szolgáló funkciók, - hozzáférési jogok kezelése.
Összeköttetés	- Tárhelyfunkciók és interfészek más hálózatokhoz és szolgáltatásokhoz.
Menedzselt hálózati szolgáltatások	- Hálózati szolgáltatások nyilvántartásba vétele és engedélyezése, - kommunikációs, hely- és forgalmi adatok tárolása és feldolgozása, - a hálózat és hálózati funkciók külső alkalmazásoknak és szolgáltatásoknak való kitettsége.
Virtualizált hálózati funkciók (NFV) kezelése és összehangolása és hálózati összehangolás (MANO), beleértve a virtualizációs infrastruktúrát is	- Az NFV összehangolásának és konfigurálásának irányítási funkciói a megvalósítás típusától függetlenül (VM, konténer, mikroszolgáltatások), - virtualizációs funkciók az NFV megvalósításához és használatához, - Hálózati szeletválasztási funkció (NSSF).
Rádió-hozzáférési hálózat	- Az 5G vagy fejlettebb technológiát támogató bázisállomások.
Irányítási rendszerek és egyéb támogató rendszerek	- A mobil kommunikációs hálózat működésének és kezelésének nyomon követése, beleértve a hozzáférési részt (RAN/O-RAN), - biztonsági események, anomáliák, fenyegetések felderítésére és a kezelésükre szolgáló rendszerek (biztonsági funkciók, beleértve a SIEM/SOAR-t).
Jogszerű lehallgatás	- Az illetékes hatóság által a kommunikációs tartalomhoz és a felhasználói forgalomra vonatkozó adatokhoz való hozzáférés funkciói.