## SEKTOROVÉ BEZPEČNOSTNÉ OPATRENIA V OBLASTI KYBERNETICKEJ BEZPEČNOSTI V ŽELEZNIČNEJ DOPRAVE

| Položka | Organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti podľa § 20 ods. 2 písm. a) zákona sa prijme tak, že | Relevancia pre IKT* | | Relevancia pre OT* | |
|---|---|---|---|---|---|
| | | PZS* | PKZS* | PZS* | PKZS* |
| 1. | manažér kybernetickej bezpečnosti predkladá návrhy bezpečnostných opatrení a oznamuje informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa železničnej infraštruktúry alebo železničného podniku | ÁNO | ÁNO | ÁNO | ÁNO |
| 2. | je určená osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému v oblasti železničnej dopravy a za prideľovanie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a informačného systému v oblasti železničnej dopravy podľa príslušnej bezpečnostnej politiky | ÁNO | ÁNO | ÁNO | ÁNO |
| 3. | je definovaná a schválená štruktúra pre zavedenie, prevádzku a riadenie kybernetickej bezpečnosti vrátane pridelenia úloh, rolí, ako aj určenie zodpovedností podľa právomocí na schvaľovanie bezpečnostných opatrení, dohľad, kontrolu, audit a vzdelávanie | ÁNO | ÁNO | ÁNO | ÁNO |
| 4. | je zabezpečená primeranosť zdrojov na riadenie kybernetickej bezpečnosti a vzdelávanie v oblasti kybernetickej bezpečnosti pre systémy riadenia vlakovej dopravy, informačné systémy železničného podniku a kritické prevádzkové technológie železničnej infraštruktúry | ÁNO | ÁNO | ÁNO | ÁNO |
| 5. | je definovaný a zavedený systém vzdelávania a preškoľovania pre všetky roly týkajúce sa kybernetickej bezpečnosti v sektore železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 6. | je uplatnená zásada najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v najväčšom rozsahu potrebnom na splnenie pridelených úloh | ÁNO | ÁNO | ÁNO | ÁNO |
| 7. | je uplatnená zásada oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie upravovať alebo používať aktíva prevádzkovateľa železničnej infraštruktúry alebo železničného podniku bez autorizácie alebo overenia identity | ÁNO | ÁNO | ÁNO | ÁNO |
| 8. | sú uplatnené zásady vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 9. | je uplatnená zásada sprístupňovania informácií podľa zásady aktuálnej potreby poznať, podľa ktorej prístup k informáciám a ich vlastníctvo je obmedzené len na tie osoby, ktoré z dôvodu plnenia svojich úloh alebo povinností musia byť s takýmito informáciami oboznámené alebo ich spracúvajú | ÁNO | ÁNO | ÁNO | ÁNO |
| 10. | štatutárny orgán sa preukázateľne zaväzuje dodržiavať povinnosti v oblasti kybernetickej bezpečnosti v súlade so stratégiou kybernetickej bezpečnosti a určenými bezpečnostnými politikami a postupmi uplatniteľnými pre sektor železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 11. | je definovaný, schválený a zavedený vnútorný kontrolný systém pre oblasť kybernetickej bezpečnosti v sektore železničnej dopravy umožňujúci včasné odhaľovanie nedostatkov | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Správa zraniteľností a kybernetických hrozieb podľa § 20 ods. 2 písm. b) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 12. | je zabezpečená informovanosť o identifikovaných kybernetických hrozbách s cieľom prijať primerané bezpečnostné opatrenia vrátane kybernetických hrozieb špecifických pre informačné a komunikačné technológie a operačné technológie železničnej infraštruktúry a železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 13. | sú získavané informácie o zraniteľnostiach používaných informačných systémov železničnej dopravy vrátane hodnotenia, do akej miery sú tieto systémy zraniteľné, posudzovania z hľadiska vplyvu na železničnú dopravu a prijímania primeraných opatrení na ich mitigáciu | ÁNO | ÁNO | ÁNO | ÁNO |
| 14. | je najmenej raz ročne vykonávané pravidelné posudzovanie zraniteľností informačných systémov železničnej dopravy a operačných technológií železničnej prevádzky | ÁNO | - | ÁNO | ÁNO |
| 15. | je najmenej raz za šesť mesiacov vykonávané pravidelné posudzovanie zraniteľností kritických systémov v sektore železničnej dopravy | - | ÁNO | - | - |
| 16. | sú určené priority aktualizácií na základe posúdenia rizík a analýzy vplyvov na bezpečnosť a kontinuitu železničnej infraštruktúry a železničnej prevádzky | ÁNO | ÁNO | ÁNO | ÁNO |
| 17. | na webovom sídle sú zverejnené kontaktné údaje pre nahlasovanie zistených zraniteľností | - | ÁNO | - | ÁNO |
| **Položka** | **Správa aktív a riadenie kybernetických hrozieb a rizík podľa § 20 ods. 2 písm. c) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 18. | sú zdokumentované a prijaté pravidlá používania a postupy nakladania s aktívami využívanými v sektore železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 19. | zamestnanci prevádzkovateľa železničnej dopravy alebo železničného podniku a zamestnanci tretích strán pri zmene alebo pri ukončení pracovného pomeru, zmluvy alebo obdobného zmluvného vzťahu preukázateľným spôsobom vracajú prevádzkovateľovi železničnej dopravy alebo železničného podniku všetky aktíva, ktoré mali zverené | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Riadenie udalostí a kybernetických bezpečnostných incidentov podľa § 20 ods. 2 písm. d) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 20. | je zabezpečené plánovanie a testovanie riešenia kybernetických bezpečnostných incidentov najmenej raz ročne a sú definované, prijaté a oznámené procesy, úlohy a zodpovednosti v oblasti riešenia kybernetických bezpečnostných incidentov ovplyvňujúcich riadenie vlakovej dopravy, oznamovacie a zabezpečovacie zariadenia, vlakové zabezpečovače a systémy rádiovej kontroly, systém prenosu dát a hlasovej komunikácie a systém zabezpečenia napájania pre elektrifikované trate a železničné zariadenia | ÁNO | ÁNO | ÁNO | ÁNO |
| 21. | je zabezpečené posúdenie udalostí kybernetickej bezpečnosti a určenie ich priorít na základe ich závažnosti a vplyvu na železničnú dopravu | ÁNO | ÁNO | ÁNO | ÁNO |
| 22. | je určený zoznam priorít reakcie na kybernetické bezpečnostné incidenty v prostredí železničnej dopravy z hľadiska dostupnosti na systémy riadenia a zabezpečenia železničnej dopravy, najmä zabezpečovacie zariadenia, ETCS, dispečerské systémy, komunikačné systémy a systémy napájania | ÁNO | ÁNO | ÁNO | ÁNO |
| 23. | je definovaný systém reakcie na kybernetické bezpečnostné incidenty v prostredí železničnej dopravy podľa určeného zoznamu priorít s ohľadom na ich vplyv na bezpečnosť a plynulosť železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 24. | poznatky získané z riešených kybernetických bezpečnostných incidentov sú preukázateľne zohľadnené v procese riadenia kybernetickej bezpečnosti v železničnej doprave | ÁNO | ÁNO | ÁNO | ÁNO |
| 25. | sú zavedené a uplatňované postupy na identifikáciu, zhromažďovanie, získavanie a uchovávanie digitálnych stôp súvisiacich s kybernetickými bezpečnostnými incidentmi v sektore železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 26. | v prípade kybernetického bezpečnostného incidentu sú dodržiavané všetky bezpečnostné opatrenia a postupy na ochranu železničnej infraštruktúry a železničnej dopravy smerujúce k rýchlej stabilizácii prevádzky a minimalizácii vplyvu incidentu na železničnú dopravu | ÁNO | ÁNO | ÁNO | ÁNO |
| 27. | sú definované a pravidelne, najmenej raz ročne testované pravidlá pre izoláciu kritických komponentov sietí | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| | železničnej infraštruktúry a železničnej dopravy, informačných systémov železničnej infraštruktúry a železničnej dopravy a operačných technológií železničnej infraštruktúry a železničnej dopravy počas kybernetického bezpečnostného incidentu; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia | | | | |
| **Položka** | **Riadenie kontinuity činností, zálohovanie, obnova systémov po havárii a krízové riadenie podľa § 20 ods. 2 písm. e) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 28. | sú prijímané opatrenia tak, aby bola dostupnosť aktív počas kybernetického bezpečnostného incidentu primerane zabezpečená plánovaním, prijatím, udržiavaním a testovaním na základe cieľov procesu riadenia kontinuity činností a požiadaviek na obnovu prevádzky informačných technológií alebo operačných technológií železničnej infraštruktúry a železničnej dopravy po kybernetickom bezpečnostnom incidente | ÁNO | ÁNO | ÁNO | ÁNO |
| 29. | sú udržiavané a pravidelne, najmenej raz ročne testované záložné kópie dát, softvéru a konfigurácie sietí, informačných systémov a operačných technológií železničnej infraštruktúry a železničnej dopravy; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia | ÁNO | ÁNO | ÁNO | ÁNO |
| 30. | infraštruktúra sietí, informačných systémov a operačných technológií železničnej infraštruktúry a železničnej dopravy je zriadená s dostatočnou redundanciou s cieľom zachovania bezpečnosti a plynulosti železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 31. | komponenty operačných technológií sietí sú schopné prepínať sa na núdzové napájanie a z núdzového napájania bez vplyvu na aktuálny stav zabezpečenia alebo na vopred definovaný obmedzený režim | - | - | ÁNO | ÁNO |
| 32. | je zavedený a dodržiavaný princíp ukladania záloh do logicky, fyzicky a geograficky oddelených priestorov | ÁNO | - | ÁNO | - |
| 33. | je zavedený a dodržiavaný princíp spravovania záložných kópií údajov alebo konfigurácií, ktorý zabezpečuje tri kópie údajov alebo konfigurácií na dvoch rozličných typoch médií, z ktorých jedna kópia je uložená v logicky, fyzicky a geograficky oddelenom priestore | - | ÁNO | - | ÁNO |
| 34. | zálohy týkajúce sa operačných technológií sietí sú oddelené v samostatnom zálohovacom systéme | - | - | - | ÁNO |
| 35. | pre zálohy týkajúce sa operačných technológií sietí železničnej infraštruktúry a železničnej dopravy je najmenej raz ročne vykonávaná kontrola funkčnosti záloh aspoň dvoch rôznych systémov; o kontrole funkčnosti | - | - | - | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| | záloh sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia | | | | |
| **Položka** | **Bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií podľa § 20 ods. 2 písm. f) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 36. | je zabezpečené prepojenie procesov riadenia rizík a projektového riadenia počas celého životného cyklu projektov železničnej infraštruktúry a železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 37. | sú prijaté opatrenia na zabránenie strate, poškodeniu, krádeži alebo kompromitácii aktív a prerušeniu prevádzky | ÁNO | ÁNO | ÁNO | ÁNO |
| 38. | prístup k zdrojovému kódu, vývojovým technológiám a softvérovým knižniciam na čítanie a zápis je riadený | ÁNO | ÁNO | ÁNO | ÁNO |
| 39. | sú prijaté bezpečnostné opatrenia s požadovanými bezpečnostnými nastaveniami tak, aby konfigurácia technických prostriedkov, programových prostriedkov, služieb a sietí nebola zmenená neoprávnenými osobami | ÁNO | ÁNO | ÁNO | ÁNO |
| 40. | sú odinštalované alebo zakázané služby neslúžiace na vykonávanie činností prevádzkovateľa železničnej dopravy alebo železničného podniku na podporných aktívach v sektore železničnej dopravy | - | ÁNO | - | ÁNO |
| 41. | je zabezpečený prístup do systémov len prostredníctvom silnej autentifikácie, minimálne dvojfaktorovým overovaním (použitie najmenej dvoch nezávislých vzájomne sa nekompromitujúcich autentifikačných prvkov zabezpečujúcich vysokú úroveň ochrany) | - | ÁNO | - | - |
| 42. | sú určené a aplikované základné parametre pre bezpečné konfigurácie operačných technológií železničnej prevádzky | - | - | ÁNO | ÁNO |
| 43. | komponenty operačných technológií železničnej prevádzky sú konfigurované podľa odporúčaných bezpečnostných nastavení uvedených dodávateľom komponentu operačných technológií v sektore železničnej dopravy | - | - | ÁNO | ÁNO |
| 44. | komponenty operačných technológií železničnej prevádzky poskytujú rozhranie na prístup k aktuálne nasadeným bezpečnostným konfiguračným nastaveniam | - | - | ÁNO | ÁNO |
| 45. | je pravidelne, najmenej raz ročne vykonávaná kontrola a aktualizácia konfigurácie komponentov sietí železničnej infraštruktúry a železničnej dopravy, informačných systémov železničnej infraštruktúry a železničnej dopravy a operačných technológií železničnej infraštruktúry a železničnej dopravy podľa vývoja hrozieb; o kontrole sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 46. | sú určené a uplatnené pravidlá bezpečného vývoja softvéru a informačných systémov v sektore železničnej dopravy využívaných pri riadení, zabezpečení a prevádzke železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 47. | sú pri vývoji alebo získavaní aplikácií identifikované a naplnené relevantné požiadavky na kybernetickú bezpečnosť | ÁNO | ÁNO | - | - |
| 48. | Riadiaci systém umožňuje zabrániť ďalšiemu prístupu spustením uzamknutia relácie po konfigurovateľnom čase nečinnosti alebo manuálnym uzamknutím; blokovanie relácie zostáva v platnosti, ak používateľ, ktorý reláciu vlastní, alebo iný oprávnený používateľ neobnoví prístup pomocou schválených identifikačných a autentifikačných postupov – toto opatrenie je relevantné pre operačné technológie železničnej prevádzky priamo ovplyvňujúce riadenie, bezpečnosť a plynulosť vlakovej prevádzky | - | - | ÁNO | ÁNO |
| 49. | je zavedená a dodržiavaná schopnosť chrániť integritu relácií v informačných systémoch a operačných technológiách železničnej infraštruktúry a železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 50. | je automaticky odmietnuté použitie neplatných identifikátorov relácií v informačných systémoch a operačných technológiách železničnej infraštruktúry a železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 51. | je zaručený bezpečný návrh, inštalácia a prevádzka sietí, informačných systémov a operačných technológií železničnej infraštruktúry a železničnej dopravy v rámci životného cyklu | ÁNO | ÁNO | ÁNO | ÁNO |
| 52. | v rámci životného cyklu vývoja operačných technológií železničnej infraštruktúry a železničnej dopravy sú návrhy a zmeny vykonané vo vyhradenom vývojovom prostredí | - | - | ÁNO | ÁNO |
| 53. | sú definované a vykonávané procesy súvisiace s bezpečným programovaním softvéru s cieľom znížiť počet potenciálnych zraniteľností v softvéri | ÁNO | ÁNO | ÁNO | ÁNO |
| 54. | sú definované a vykonávané procesy testovania bezpečnosti informačných systémov a operačných technológií železničnej infraštruktúry a železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 55. | testovanie kybernetickej bezpečnosti je začlenené do životného cyklu vývoja a údržby sietí, informačných systémov a operačných technológií železničnej infraštruktúry a železničnej dopravy využívaných pri riadení a zabezpečení železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 56. | sú riadené, monitorované a kontrolované činnosti súvisiace s vývojom programových prostriedkov a informačných systémov železničnej infraštruktúry a železničnej dopravy, ktoré sú dodávané treťou stranou | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 57. | vývojové, testovacie a produkčné prostredia sú vzájomne oddelené a zabezpečené | ÁNO | ÁNO | ÁNO | ÁNO |
| 58. | dáta používané pre testovanie systémov železničnej dopravy sú vhodne vyberané, chránené a spravované | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti podľa § 20 ods. 2 písm. g) zákona sa prijmú tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 59. | je zaručený súlad s požiadavkami vyplývajúcimi zo všeobecne záväzných právnych predpisov a zmluvnými požiadavkami týkajúcimi sa kybernetickej bezpečnosti v sektore železničnej dopravy | ÁNO | ÁNO | - | - |
| 60. | riadenie kybernetickej bezpečnosti je nezávisle prehodnocované v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií | ÁNO | ÁNO | ÁNO | ÁNO |
| 61. | súlad so stratégiou kybernetickej bezpečnosti, bezpečnostnými politikami, bezpečnostnými štandardmi a normami je prehodnocovaný najmenej raz ročne v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií | ÁNO | ÁNO | ÁNO | ÁNO |
| 62. | sú definované pravidlá pre výkon auditných činností a kontrolných činností v oblasti kybernetickej bezpečnosti v sektore železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Kryptografické opatrenia a zásady používania kryptografie podľa § 20 ods. 2 písm. h) zákona sa prijmú tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 63. | nastavením pravidiel pre použitie vhodných kryptografických metód je obmedzené potenciálne narušenie dôvernosti informácií vrátane osobných údajov a prevádzkových údajov železničnej dopravy a sú dodržiavané požiadavky vyplývajúce zo všeobecne záväzných právnych predpisov, požiadavky vyplývajúce zo zmlúv alebo v prípade certifikovaného subjektu normatívne požiadavky týkajúce sa kybernetickej bezpečnosti | ÁNO | ÁNO | ÁNO | ÁNO |
| 64. | sú definované a zavedené pravidlá efektívneho používania kryptografických mechanizmov vrátane správy kryptografických kľúčov a postupov | ÁNO | ÁNO | ÁNO | ÁNO |
| 65. | sú prijaté a aplikované postupy na pravidelné prehodnocovanie odolnosti zavedených kryptografických mechanizmov; prehodnocovanie odolnosti zavedených kryptografických mechanizmov sa vykonáva najmenej raz ročne a vyhotovuje sa o tom záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Bezpečnosť a spôsobilosti ľudských zdrojov podľa § 20 ods. 2 písm. i) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |

| | | PZS* | PKZS* | PZS* | PKZS* |
|---|---|---|---|---|---|
| 66. | sú určené pravidlá pre zaradenie osôb do jednotlivých pracovných rolí v sektore železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 67. | v pracovných zmluvách, zmluvách v súvislosti s iným obdobným pracovnoprávnym vzťahom alebo iných súvisiacich dokumentoch sú uvedené zodpovednosti za kybernetickú bezpečnosť | ÁNO | ÁNO | ÁNO | ÁNO |
| 68. | pre všetky pracovné roly je poskytované primerané vzdelávanie, aby štatutárny orgán prevádzkovateľa železničnej infraštruktúry alebo železničnej dopravy, zamestnanci a tretie strany mali primerané povedomie o kybernetickej bezpečnosti v oblasti informačných a operačných technológií železničnej dopravy; súčasťou školení sú aj praktické simulácie a cvičenia reakcie na kybernetické bezpečnostné incidenty | ÁNO | ÁNO | ÁNO | ÁNO |
| 69. | zamestnanci prevádzkovateľa železničnej infraštruktúry alebo železničnej dopravy a tretie strany sú preukázateľne oboznámení s bezpečnostnými politikami | ÁNO | ÁNO | ÁNO | ÁNO |
| 70. | aktualizované verzie bezpečnostných politík sú bezodkladne sprístupňované vrcholovému vedeniu prevádzkovateľa železničnej infraštruktúry alebo železničnej dopravy, manažmentu prevádzkovateľa železničnej infraštruktúry alebo železničnej dopravy, zamestnancom prevádzkovateľa železničnej infraštruktúry alebo železničnej dopravy a v potrebnom rozsahu aj tretej strane alebo ďalším zainteresovaným stranám | ÁNO | ÁNO | ÁNO | ÁNO |
| 71. | sú formalizované disciplinárne procesy voči zamestnancom prevádzkovateľa železničnej infraštruktúry alebo železničného podniku, ktorí sa dopustili porušenia ustanovení bezpečnostných politík prevádzkovateľa železničnej infraštruktúry alebo železničného podniku | ÁNO | ÁNO | ÁNO | ÁNO |
| 72. | zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti, ktoré zostávajú v platnosti aj pri zmene alebo pri ukončení pracovnoprávneho vzťahu alebo zmluvy tretej strany s prevádzkovateľom základnej služby podľa § 19 ods. 2 zákona, sú v rámci zmeny alebo ukončenia pracovnoprávneho vzťahu alebo zmluvy tretej strany s prevádzkovateľom základnej služby podľa § 19 ods. 2 zákona definované, presadzované a oznámené príslušným zamestnancom, tretím stranám alebo iným zainteresovaným stranám s cieľom chrániť záujmy prevádzkovateľa železničnej infraštruktúry alebo železničného podniku | ÁNO | ÁNO | ÁNO | ÁNO |
| 73. | sú určené, zdokumentované a pravidelne, najmenej raz za dva roky, preskúmavané a podpisované dohody o mlčanlivosti, ktoré odrážajú potreby prevádzkovateľa železničnej infraštruktúry a železničného podniku pre zachovanie dôvernosti | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 74. | ak zamestnanci pracujú na diaľku, sú prijaté bezpečnostné opatrenia na ochranu informácií, ku ktorým sa pristupuje, ktoré sa spracúvajú alebo ktoré sa uchovávajú mimo priestorov prevádzkovateľa železničnej infraštruktúry alebo železničného podniku | ÁNO | ÁNO | ÁNO | ÁNO |
| 75. | sa používa viacfaktorové overovanie pre vzdialený prístup do informačných systémov železničnej dopravy a operačných technológií železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 76. | sú prijaté požiadavky na identifikáciu oprávnenosti pristupujúceho technického prostriedku a následne aj používateľa; toto opatrenie je relevantné pre operačné technológie železničnej dopravy | - | - | ÁNO | ÁNO |
| 77. | v prípade prístupu na inžinierske prostredia v rámci prostredia operačných technológií železničnej dopravy je zaistený prístup a overenie technológiou pre záznam a archiváciu úkonov externej organizácie; toto opatrenie je relevantné pre operačné technológie železničnej dopravy | - | - | - | ÁNO |
| **Položka** | **Správa identít a prístupov podľa § 20 ods. 2 písm. j) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 78. | pri riadení prístupov k sieťam a informačným systémom železničnej infraštruktúry a železničnej dopravy sú využívané technológie na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a technológie na riadenie prístupových oprávnení, prostredníctvom ktorých je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie údajov a zápis údajov a na zmeny oprávnení a prostredníctvom ktorých sa zaznamenáva použitie prístupových oprávnení | ÁNO | ÁNO | ÁNO | ÁNO |
| 79. | je zavedená a využívaná samostatná oddelená technológia na riadenie prístupov v operačných technológiách železničnej dopravy | - | - | - | ÁNO |
| 80. | je zaručené riadenie jednoznačných identifikátorov používateľov a systémov vrátane prístupových práv a oprávnení používateľských účtov a systémových účtov počas celého životného cyklu identít | ÁNO | ÁNO | ÁNO | ÁNO |
| 81. | každému používateľovi a systémovému účtu je pridelený jednoznačný identifikátor na autentizáciu na prístup do siete a informačného systému železničnej infraštruktúry a železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 82. | v pravidelných intervaloch, najmenej raz ročne, je vykonávaná kontrola prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom vykonávania oprávnení vrátane detekcie a následného zneplatnenia nepoužívaných prístupových účtov; vyhotovuje sa o tom záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| | auditu do ukončenia nasledujúceho auditu alebo samohodnotenia | | | | |
| 83. | je zavedené riadenie prístupov na základe rolí a zásady najnižších oprávnení pre používateľov informačných systémov a operačných technológií železničnej dopravy | - | ÁNO | ÁNO | ÁNO |
| 84. | privilegované prístupové práva sú poskytované len oprávneným používateľom prostredníctvom komponentov informačných a operačných technológií riadenia železničnej dopravy a službám podľa príslušnej politiky riadenia prístupov a práv | ÁNO | ÁNO | ÁNO | ÁNO |
| 85. | prístup k aktívam je obmedzený v súlade s určenou a definovanou politikou riadenia prístupov | ÁNO | ÁNO | ÁNO | ÁNO |
| 86. | technológie a postupy bezpečnej autentizácie sú zavedené na základe požiadaviek na obmedzenie prístupu k informáciám podľa príslušnej politiky riadenia prístupov a práv | ÁNO | ÁNO | ÁNO | ÁNO |
| 87. | používatelia majú prijaté primerané opatrenia na ochranu a udržiavanie pridelených autentifikačných prostriedkov vrátane nezdieľania autentifikačných prostriedkov s inými osobami | ÁNO | ÁNO | ÁNO | ÁNO |
| 88. | všetky prístupy do sietí, informačných systémov a operačných technológií železničnej infraštruktúry a železničnej dopravy z nedôveryhodných zdrojov sú riadené a monitorované | - | - | ÁNO | ÁNO |
| 89. | siete, informačné systémy a operačné technológie železničnej infraštruktúry a železničnej dopravy umožňujú identifikáciu neoprávnených rádiofrekvenčných zariadení | - | ÁNO | - | ÁNO |
| **Položka** | **Bezpečnosť pri prevádzke sietí a informačných systémov podľa § 20 ods. 2 písm. k) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 90. | prevádzkové postupy pre zariadenia na spracovanie informácií, siete a informačné systémy železničnej infraštruktúry a železničnej dopravy sú zdokumentované a sprístupnené zamestnancom podľa ich potreby | ÁNO | ÁNO | ÁNO | ÁNO |
| 91. | sa zabraňuje strate, poškodeniu alebo ohrozeniu aktív alebo prerušeniu prevádzky v dôsledku zlyhania a narušenia podporných služieb vrátane dodávky elektrickej energie | ÁNO | ÁNO | ÁNO | ÁNO |
| 92. | sa zabraňuje strate, poškodeniu, krádeži alebo kompromitácii aktív alebo prerušeniu prevádzky v súvislosti s narušením kabeláže elektrického napájania alebo dátových liniek | ÁNO | ÁNO | ÁNO | ÁNO |
| 93. | sa zabraňuje úniku informácií zo zariadení, ktoré sa majú zlikvidovať alebo opätovne použiť; všetky prvky zariadení obsahujúce pamäťové médiá sa kontrolujú, čím sa zabezpečí, že informácie a licencovaný softvér sú bezpečne zmazané alebo prepísané | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 94. | je dostupná kapacita podporných aktív potrebných na bezpečnú prevádzku železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 95. | systémový čas príslušných podporných aktív železničnej infraštruktúry a železničnej dopravy, ktoré spracúvajú informácie alebo podporujú ich spracovanie, je synchronizovaný so schválenými zdrojmi času zohľadňujúcimi časové zóny | ÁNO | ÁNO | ÁNO | ÁNO |
| 96. | používanie systémových obslužných programových prostriedkov, ktoré môžu byť schopné obísť systémové a aplikačné opatrenia, je obmedzené a kontrolované | ÁNO | ÁNO | ÁNO | ÁNO |
| 97. | sú zavedené postupy a opatrenia na bezpečné riadenie inštalácie programových prostriedkov a informačných systémov železničnej infraštruktúry a železničnej dopravy do produkčnej prevádzky | ÁNO | ÁNO | ÁNO | ÁNO |
| 98. | zmeny procesov a systémov podliehajú schválenému procesu riadenia zmien | ÁNO | ÁNO | ÁNO | ÁNO |
| 99. | je definovaný a zavedený proces riadenia výnimiek zo schválených bezpečnostných opatrení v sektore železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Ochrana proti škodlivému kódu a nežiaducemu obsahu podľa § 20 ods. 2 písm. l) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 100. | je zavedená ochrana proti škodlivému kódu, ktorá je podporovaná primeraným budovaním povedomia používateľov | ÁNO | ÁNO | ÁNO | ÁNO |
| 101. | je zaručená pravidelná aktualizácia sietí, informačných systémov a operačných technológií železničnej infraštruktúry a železničnej dopravy s cieľom zabezpečiť minimálne narušenie prevádzky železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 102. | prístup k externým internetovým zdrojom je riadený s cieľom znížiť vystavenie škodlivému obsahu a minimalizovať riziká pre riadenie a prevádzku železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Systémová bezpečnosť, sieťová bezpečnosť a komunikačná bezpečnosť podľa § 20 ods. 2 písm. m) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 103. | sú vypracované a zavedené postupy na prenos informácií v rámci organizácie, ako aj s tretími stranami pre všetky typy technických prostriedkov a médií používaných v železničnej doprave | ÁNO | ÁNO | ÁNO | ÁNO |
| 104. | je používané šifrovanie na zabezpečenie údajov pri prenose vybraných údajov medzi systémami operačných technológií železničnej infraštruktúry a železničnej dopravy; identifikácia vybraných údajov prebieha pomocou klasifikácie informácií, pričom rozsah a spôsob | - | - | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| | šifrovania zodpovedá citlivosti údajov a požiadavkám na bezpečnosť a plynulosť železničnej dopravy | | | | |
| 105. | je používané šifrovanie na zabezpečenie vybraných údajov pri prenose medzi a v rámci rôznych úrovní systémov operačných technológií železničnej infraštruktúry a železničnej dopravy v rozsahu vyplývajúcom z posúdenia rizík a významu systémov; identifikácia vybraných údajov prebieha pomocou klasifikácie informácií | - | - | - | ÁNO |
| 106. | je zabezpečená komunikácia medzi systémami riadenia a zabezpečenia železničnej dopravy, najmä v systémoch rádiovej komunikácie alebo prenosu prevádzkových dát | - | - | - | ÁNO |
| 107. | je používané šifrovanie komunikácie medzi dispečerskými pracoviskami a traťovými systémami v rozsahu vyplývajúcom z posúdenia rizík, podľa rizika a významu systémov | - | - | - | ÁNO |
| 108. | na informačné systémy, siete a technické prostriedky, ktoré spracúvajú, uchovávajú alebo prenášajú chránené informácie, podľa klasifikácie informácií, sa aplikujú opatrenia na prevenciu úniku informácií vrátane zohľadnenia proprietárnych protokolov a dátových tokov; identifikácia vybraných informácií prebieha pomocou klasifikácie informácií | ÁNO | ÁNO | ÁNO | ÁNO |
| 109. | siete a technické prostriedky komunikačných sietí železničnej infraštruktúry a železničnej dopravy sa zabezpečujú, spravujú a kontrolujú s cieľom chrániť informácie v informačných systémoch a programových prostriedkoch | ÁNO | ÁNO | ÁNO | ÁNO |
| 110. | sú určené, zavedené a monitorované bezpečnostné funkcie, úrovne služieb a požiadavky týkajúce sa sieťových služieb | ÁNO | ÁNO | ÁNO | ÁNO |
| 111. | sú prijaté a udržiavané systémy detekcie narušenia, ktoré zohľadňujú proprietárne protokoly a dátové toky používané v sektore železničnej dopravy | - | - | ÁNO | ÁNO |
| 112. | pre komponenty operačných technológií je automaticky ukončovaná vzdialená relácia po určenom konfigurovateľnom čase nečinnosti | - | - | ÁNO | ÁNO |
| 113. | je definovaná a zavedená segmentácia sietí, pričom informačné systémy so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente sú len informačné systémy s podobným účelom | ÁNO | ÁNO | ÁNO | ÁNO |
| 114. | sú prijaté a udržiavané mechanizmy na smerovanie a filtráciu sieťovej prevádzky do a z externých sietí cez sieťový firewall | - | - | ÁNO | ÁNO |
| 115. | je definovaná a zavedená logická segmentácia medzi operačnými technológiami, sieťami a informačnými systémami | - | - | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 116. | je zavedená fyzická a logická segmentácia medzi riadiacimi systémami dopravy a ostatnými sieťami | - | - | - | ÁNO |
| 117. | sú segmentované vybrané siete riadiaceho systému železničnej dopravy od ostatných sietí operačných technológií | - | - | ÁNO | ÁNO |
| 118. | sieťový firewall pre operačné technológie železničnej dopravy je nezávislý od ostatných mechanizmov na smerovanie a filtráciu sieťovej prevádzky | - | - | ÁNO | ÁNO |
| 119. | v sieťach určených pre operačné technológie železničnej dopravy je blokované odosielanie a prijímanie správ medzi používateľmi | - | - | ÁNO | ÁNO |
| **Položka** | **Monitorovanie, zaznamenávanie a hlásenie udalostí podľa § 20 ods. 2 písm. n) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 120. | sú vytvárané a najmenej jeden rok uchovávané relevantné prevádzkové a bezpečnostné logy, ktoré zachytávajú činnosti, výnimky, poruchy a iné relevantné prevádzkové a bezpečnostné udalosti v systémoch železničnej infraštruktúry a železničnej dopravy, pričom sa zabráni zmene ich integrity a neoprávneným prístupom k nim | ÁNO | ÁNO | ÁNO | ÁNO |
| 121. | záznamy o činnostiach obsahujú informáciu o pôvodcovi vykonanej činnosti | - | ÁNO | - | ÁNO |
| 122. | je zavedený systém monitorovania, ktorý zaznamenáva udalosti v reálnom čase | - | ÁNO | - | ÁNO |
| 123. | siete, informačné systémy, programové prostriedky a aplikácie sú monitorované z hľadiska nezvyčajného správania a sú prijaté vhodné opatrenia na vyhodnotenie kybernetických bezpečnostných udalostí | ÁNO | ÁNO | ÁNO | ÁNO |
| 124. | siete, informačné systémy, programové prostriedky a aplikácie sú monitorované z hľadiska nezvyčajného správania a sú prijaté vhodné opatrenia na vyhodnotenie kybernetických bezpečnostných udalostí automatizovaným spôsobom | - | ÁNO | - | ÁNO |
| 125. | sú prijaté a udržiavané mechanizmy overovania činností bezpečnostných funkcií a oznamovania nezvyčajného správania počas bežnej prevádzky, testovania a plánovanej údržby systémov železničnej infraštruktúry a železničnej dopravy | - | - | ÁNO | ÁNO |
| **Položka** | **Fyzická bezpečnosť, bezpečnosť prostredia a správa koncových zariadení podľa § 20 ods. 2 písm. o) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 126. | sú definované a používané bezpečnostné perimetre na ochranu oblastí, ktoré obsahujú aktíva používané v sieťach, informačných systémoch a operačných technológiách | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 127. | priestory, v ktorých sa nachádzajú riadiace a serverové súčasti informačných a operačných technológií železničnej infraštruktúry a železničnej dopravy, majú definované pravidlá fyzickej bezpečnosti | ÁNO | ÁNO | ÁNO | ÁNO |
| 128. | fyzický prístup k vybraným aktívam infraštruktúry, ktoré sú klasifikované ako kritické alebo významné z hľadiska bezpečnosti a prevádzky, je povolený výhradne autorizovaným osobám | ÁNO | ÁNO | ÁNO | ÁNO |
| 129. | je navrhnutá a zavedená fyzická bezpečnosť kancelárií, miestností a zariadení | ÁNO | ÁNO | ÁNO | ÁNO |
| 130. | zabezpečené priestory sú nepretržite monitorované z hľadiska neoprávneného fyzického prístupu | ÁNO | ÁNO | ÁNO | ÁNO |
| 131. | sú monitorované všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu | ÁNO | ÁNO | ÁNO | ÁNO |
| 132. | je navrhnutá a zavedená ochrana pred fyzickými hrozbami a environmentálnymi hrozbami, ako sú prírodné katastrofy a iné úmyselné alebo neúmyselné ohrozenia informačných a operačných technológií železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 133. | aktíva v zabezpečených priestoroch sú chránené pred poškodením a neoprávneným zásahom zo strany zamestnancov pracujúcich v týchto priestoroch a nepovolaných osôb | ÁNO | ÁNO | ÁNO | ÁNO |
| 134. | sú definované a primerane presadzované pravidlá čistého stola pre listinné dokumenty a prenosné pamäťové médiá a pravidlá pre čisté obrazovky zariadení na spracovanie informácií | ÁNO | ÁNO | ÁNO | ÁNO |
| 135. | sú riadené riziká vyplývajúce z hrozieb fyzického prostredia a z neoprávneného fyzického prístupu k aktívam | ÁNO | ÁNO | ÁNO | ÁNO |
| 136. | sa prijímajú opatrenia na zabránenie strate, poškodeniu, krádeži alebo kompromitácii zariadení používaných, prenášaných a uchovávaných mimo pracoviska a sú definované postupy, ak k takejto udalosti dôjde | ÁNO | ÁNO | ÁNO | ÁNO |
| 137. | je regulované alebo zakázané používanie prenosných zariadení v kritických oblastiach operačných technológií železničnej dopravy | - | - | ÁNO | ÁNO |
| 138. | je zabezpečené automatické presadzovanie konfigurovateľných obmedzení používania, ktoré zahŕňajú najmä zabránenie používaniu prenosných a mobilných zariadení, vyžadovanie autorizácie špecifickej pre daný kontext, obmedzenie prenosu kódu a údajov do/z prenosných a mobilných zariadení | - | - | - | ÁNO |
| 139. | je zabezpečené overenie, či prenosné alebo mobilné zariadenia, ktoré sa pokúšajú pripojiť k bezpečnostnej zóne, spĺňajú bezpečnostné požiadavky danej bezpečnostnej zóny | - | - | - | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 140. | pamäťové médiá sú riadené počas ich životného cyklu, t. j. počas ich získavania, používania, prepravy a likvidácie, v súlade s klasifikačnou schémou a požiadavkami na manipuláciu s nimi | ÁNO | ÁNO | ÁNO | ÁNO |
| 141. | dáta uložené v koncových zariadeniach používateľov, spracúvané týmito zariadeniami alebo prístupné prostredníctvom nich, sú chránené aj pri použití v prevádzke | ÁNO | ÁNO | ÁNO | ÁNO |
| 142. | informácie uložené v informačných systémoch, zariadeniach alebo na iných pamäťových médiách sú vymazané, ak už nie sú potrebné | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Ochrana záznamov, súkromia a označovanie informácií podľa § 20 ods. 2 písm. p) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 143. | informácie sú klasifikované na základe potrieb prevádzkovateľa železničnej infraštruktúry alebo železničného podniku na základe požiadaviek na dôvernosť, integritu, dostupnosť a špecifických požiadaviek zainteresovaných strán | ÁNO | ÁNO | ÁNO | ÁNO |
| 144. | dátové toky medzi jednotlivými bezpečnostnými zónami v rámci topológie systémov operačných technológií železničnej dopravy sú klasifikované na základe potrieb prevádzkovateľa železničnej infraštruktúry alebo železničného podniku a na základe požiadaviek na dôvernosť, integritu, dostupnosť a špecifických požiadaviek zainteresovaných strán | - | - | ÁNO | ÁNO |
| 145. | sú vypracované a zavedené postupy na označovanie informácií v súlade s prijatou klasifikačnou schémou | ÁNO | ÁNO | ÁNO | ÁNO |
| 146. | je zabezpečený súlad so všeobecne záväznými právnymi predpismi a zmluvnými požiadavkami týkajúcimi sa práv duševného vlastníctva a používania patentovaných produktov | ÁNO | ÁNO | ÁNO | ÁNO |
| 147. | záznamy sú primerane chránené pred stratou, zničením, falšovaním, neoprávneným prístupom a neoprávneným zverejnením | ÁNO | ÁNO | ÁNO | ÁNO |
| 148. | je zabezpečené plnenie požiadaviek týkajúcich sa ochrany osobných údajov podľa osobitných predpisov a zmluvných požiadaviek | ÁNO | ÁNO | ÁNO | ÁNO |
| **Položka** | **Dodávateľský reťazec podľa § 20 ods. 2 písm. q) zákona sa prijme tak, že** | **Relevancia pre IKT*** | | **Relevancia pre OT*** | |
| | | **PZS*** | **PKZS*** | **PZS*** | **PKZS*** |
| 149. | sú definované a zavedené procesy a postupy na riadenie kybernetických rizík spojených s používaním produktov, procesov alebo služieb tretích strán dodávaných pre sektor železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |

| | | | | | |
|---|---|---|---|---|---|
| 150. | na riadenie informačnej bezpečnosti a kybernetickej bezpečnosti vo vzťahoch s tretími stranami je s každou treťou stranou s významným vplyvom uzatvorená zmluva podľa § 19 ods. 2 zákona | ÁNO | ÁNO | ÁNO | ÁNO |
| 151. | uzatvoreniu zmluvy podľa § 19 ods. 2 zákona predchádza analýza rizík dodávateľských služieb alebo iných dodávateľských činností | ÁNO | ÁNO | ÁNO | ÁNO |
| 152. | súčasťou zmluvy podľa § 19 ods. 2 zákona sú bezpečnostné požiadavky špecifické pre informačné a komunikačné technológie alebo operačné technológie železničnej infraštruktúry alebo železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 153. | bezpečnostné opatrenia sú uplatnené v dodávateľskom reťazci produktov a služieb, ktorý priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov železničnej infraštruktúry a železničnej dopravy | ÁNO | ÁNO | ÁNO | ÁNO |
| 154. | sú pravidelne, najmenej raz za dva roky monitorované, preskúmavané, vyhodnocované a riadené zmeny v postupoch a v poskytovaní služieb alebo iných činností tretích strán, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov | ÁNO | ÁNO | ÁNO | ÁNO |
| 155. | sú špecifikované a zdokumentované minimálne bezpečnostné požiadavky pre používanie cloudových služieb a riadená kybernetická bezpečnosť pri používaní cloudových služieb využívaných v železničnej doprave | ÁNO | ÁNO | ÁNO | ÁNO |

**Vysvetlivky:**

* **IKT** – informačné a komunikačné technológie,
**OT** – operačné technológie,
**PKZS** – prevádzkovateľ kritickej základnej služby,
**PZS** – prevádzkovateľ základnej služby.