



Analýza rizík a dopadov (BIA)

RNDr. Daniel Schikor



Zákon č. **69/2018** Z. z. o kybernetickej bezpečnosti v zmysle vyhlášky č. **227/2025** Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.



Ako postupovať

Riadenie rizík informačnej bezpečnosti by malo byť nepretržitým procesom. V rámci tohto procesu by sa mali stanoviť vonkajšie a vnútorné súvislosti, posúdiť riziká a ošetriť riziká pomocou plánu ošetrenia rizík s cieľom realizovať odporúčania a rozhodnutia. Pri riadení rizík sa analyzuje, čo sa môže stať a aké môžu byť možné dôsledky, a až potom sa rozhodne, čo a kedy treba urobiť, aby sa riziko znížilo na prijateľnú úroveň.

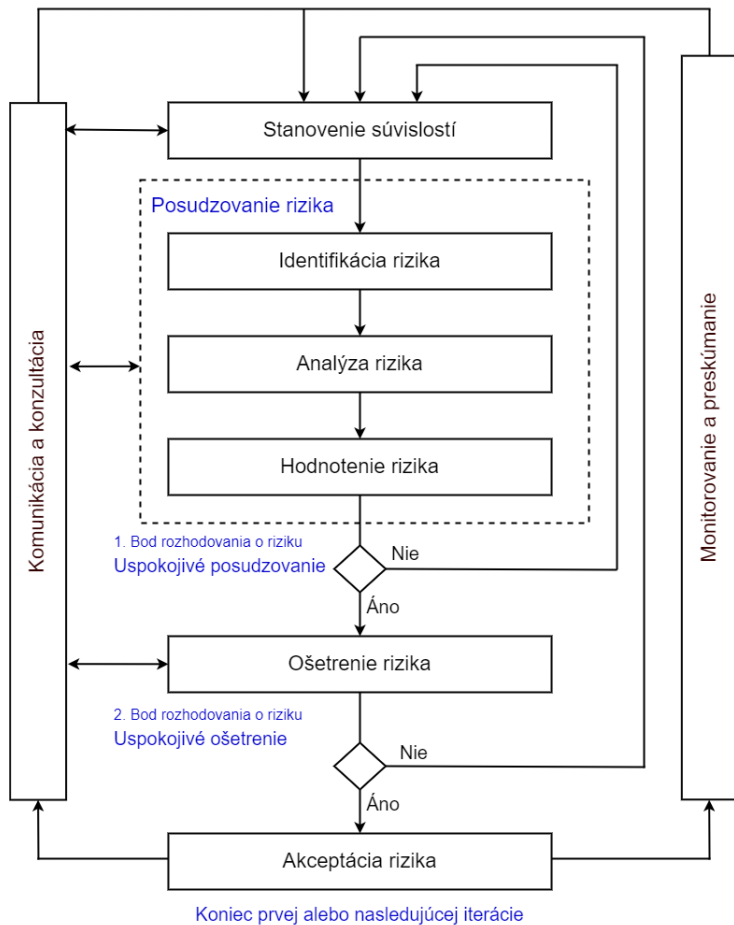


Ako postupovať

STN ISO/IEC 27005:2023



Proces riadenia rizík





Stanovenie súvislostí

Je potrebné stanoviť vonkajšie a vnútorné súvislosti pre riadenie rizík informačnej bezpečnosti, čo zahŕňa stanovenie:

- základných kritérií potrebných pre riadenie rizík informačnej bezpečnosti (kritériá hodnotenia rizík, kritériá dopadu, kritériá akceptácie rizika),
- vymedzenie rozsahu a hraníc,
- vytvorenie vhodnej organizácie, ktorá bude riadiť riziká informačnej bezpečnosti.



Posudzovanie rizika

Riziká by sa mali identifikovať, kvantifikovať alebo kvalitatívne opísať a stanoviť ich priority na základe kritérií hodnotenia rizík a cieľov relevantných pre organizáciu.

Riziko je kombináciou dôsledkov, ktoré by mohli vyplynúť z výskytu nežiaducej udalosti a pravdepodobnosti výskytu tejto udalosti.

Posúdenie rizík určuje hodnotu informačných aktív, identifikuje príslušné hrozby a zraniteľnosti, ktoré existujú (alebo môžu existovať), identifikuje existujúce opatrenia a ich vplyv na identifikované riziko.



Posudzovanie rizika

Posudzovanie rizík pozostáva z týchto činností:

- identifikácia rizík,
- analýza rizík,
- hodnotenie rizík.



Identifikácia rizík

Cieľom identifikácie rizík je určiť, čo sa môže stať, aby došlo k potenciálnej strate, a získať prehľad o tom, ako, kde a prečo môže dôjsť k strate.

Za tvorbu a prispievanie do zoznamu rizík je zodpovedný **vlastník rizika**, t. j. osoba zodpovedná za monitorovanie a riadenie všetkých aspektov konkrétneho rizika, ktoré mu bolo pridelené, vrátane implementácie vybraných opatrení určených pre hrozby.



Identifikácia rizík

Identifikácia rizík zahŕňa:

- identifikáciu aktív,
- identifikáciu hrozieb,
- identifikáciu existujúcich opatrení,
- identifikáciu zraniteľností,
- identifikáciu dôsledkov.



Identifikácia aktív

Aktívum je všetko to, čo má pre organizáciu hodnotu, a preto si vyžaduje ochranu. Pri identifikácii aktív treba mať na pamäti, že informačný systém pozostáva z viac ako len hardvéru a softvéru.

Pre každé aktívum by sa mal určiť vlastník, ktorý bude aktívum vlastniť a zodpovedať zaň. **Vlastník aktíva** možno nemá vlastnícke práva viažuce sa k aktívu, ale nesie zodpovednosť za jeho výrobu, vývoj, údržbu, používanie a bezpečnosť podľa potreby. Vlastník aktíva je často najvhodnejšou osobou na určenie hodnoty aktíva pre organizáciu.



Identifikácia hrozieb

Hrozba má potenciál poškodiť aktíva, ako sú informácie, procesy a systémy. Hrozby môžu mať prírodný alebo ľudský pôvod a môžu byť náhodné alebo úmyselné. Mali by sa identifikovať náhodné aj úmyselné zdroje hrozieb. Hrozba môže vzniknúť zvnútra alebo zvonka organizácie.

Pri aktuálnom hodnotení hrozieb by sa mali zohľadniť interné skúsenosti z incidentov a minulých posúdení hrozieb. Môže byť užitočné pozrieť si katalógy hrozieb (špecifických pre danú organizáciu alebo podnik), aby sa doplnil zoznam všeobecných hrozieb. Katalógy hrozieb a štatistiky sú k dispozícii od orgánov odvetvia, vlád, právnych orgánov, poisťovní atď.



Identifikácia existujúcich opatrení

Je potrebné vykonať identifikáciu existujúcich opatrení, aby sa predišlo zbytočnej práci alebo nákladom, napr. pri duplicite opatrení. Okrem toho by sa pri identifikácii existujúcich opatrení mala vykonať kontrola, či opatrenia fungujú správne. Ak opatrenie nefunguje podľa očakávania, môže to spôsobiť zraniteľnosť. Mala by sa zvážiť situácia, keď vybrané opatrenie (alebo stratégia) zlyháva v prevádzke, a preto sú potrebné doplnkové opatrenia na účinné riešenie identifikovaného rizika.



Identifikácia zraniteľnosti

Zraniteľnosť - slabé miesto fyzického alebo informačného aktíva, slabé miesto v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať, alebo využiť nositeľ hrozieb (resp. hrozba, škodlivá udalosť, scenár rizika).

Je potrebné identifikovať zraniteľnosti, ktoré môžu byť zneužitú hrozbami, a spôsobiť tak škody na aktívach alebo organizácii.



Identifikácia zraniteľnosti

Zraniteľnosti možno identifikovať v týchto oblastiach:

- organizácia
- procesy a postupy
- postupy riadenia
- personál
- fyzické prostredie
- konfigurácia informačného systému
- hardvér, softvér alebo komunikačné zariadenia
- závislosť od tretích strán



Identifikácia dôsledkov

Dôsledkom môže byť zníženie efektívnosti, nepriaznivé prevádzkové podmienky, strata podnikania, poškodenie dobrého mena, škoda atď.

Organizácie by mali identifikovať prevádzkové dôsledky scenárov incidentov z hľadiska:

- času vyšetrovania a opravy
- straty (pracovného) času
- stratenej príležitosti
- zdravia a bezpečnosti
- finančných nákladov na špecifické zručnosti pri odstraňovaní škôd
- povesti a dobrého mena



Analýza rizík

Analýza rizík - proces na pochopenie pôvodu rizík a zistenie úrovne rizík. Analýza rizík poskytuje základ na vyhodnotenie rizík a rozhodnutie o spôsobe ich ošetrovania.

Riziko - pravdepodobnosť, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody.



Pri analýze rizík je potrebné:

- posúdenie dôsledkov s prihliadnutím na porušenia informačnej bezpečnosti, ako je strata dôvernosti, integrity alebo dostupnosti aktív,
- posúdenie pravdepodobnosti incidentu, pritom by sa malo zohľadniť, ako často sa hrozby vyskytujú a ako ľahko sa dajú zraniteľnosti zneužiť,
- určenie úrovne rizika.



Ošetrenie rizík

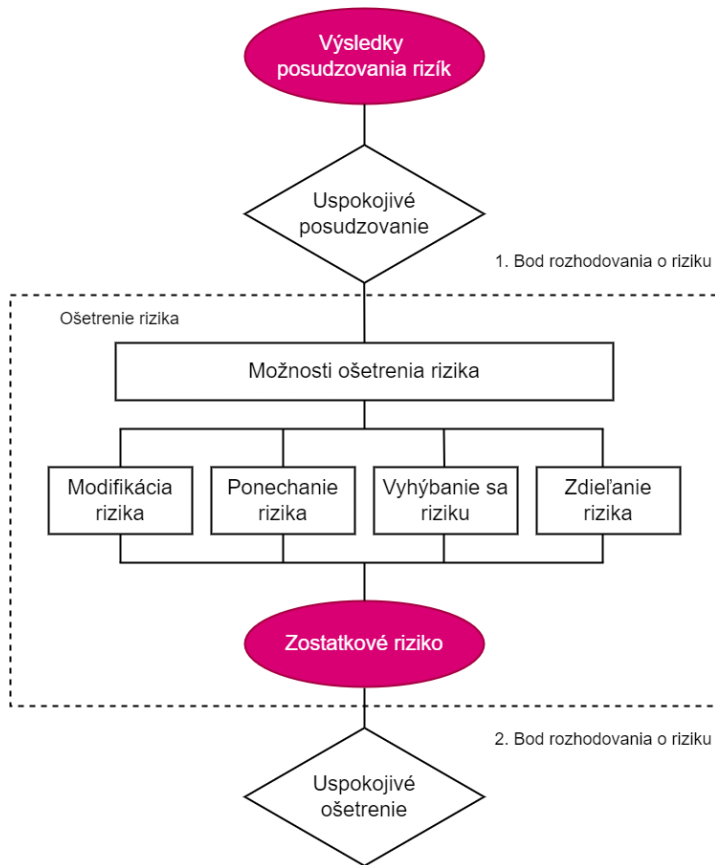
Možnosti ošetrenia rizika by sa mali vybrať na základe výsledku posúdenia rizika, očakávaných nákladov na realizáciu týchto možností a očakávaných prínosov týchto možností.

Ak je možné dosiahnuť veľké zníženie rizík pri relatívne nízkych výdavkoch, mali by sa takéto možnosti realizovať. Ďalšie možnosti zlepšenia môžu byť nevhodné a je potrebné posúdiť, či sú opodstatnené.

Mal by sa definovať plán ošetrenia rizík, v ktorom sa jasne určí poradie priorít, v ktorom by sa mali jednotlivé ošetrenia rizík realizovať, a ich časový rámec.



Ošetrenie rizík





Modifikácia (zníženie) rizika

Úroveň rizika by sa mala riadiť zavedením, odstránením alebo zmenou opatrení tak, aby sa zvyškové riziko mohlo prehodnotiť ako prijateľné.

Pri výbere opatrení je dôležité zvážiť náklady na obstaranie, implementáciu, správu, prevádzku, monitorovanie a údržbu opatrení v porovnaní s hodnotou chránených aktív.



Ošetrenie rizík

Ponechanie rizika

Ak úroveň rizika spĺňa kritériá akceptácie rizika, nie je potrebné zavádzať ďalšie opatrenia a riziko možno ponechať.



Vyhýbanie sa riziku

Ak náklady na realizáciu možností ošetrenia rizík prevyšujú prínosy, možno sa rozhodnúť, že sa riziku úplne vyhneme, a to odstúpením od plánovanej alebo existujúcej činnosti alebo súboru činností, alebo zmenou podmienok, za ktorých sa činnosť vykonáva. Napríklad v prípade rizík spôsobených prírodou môže byť nákladovo najefektívnejšou alternatívou fyzické premiestnenie zariadení na spracovanie informácií na miesto, kde riziko neexistuje alebo je pod kontrolou.



Zdieľanie rizika

Zdieľanie rizík zahŕňa rozhodnutie zdieľať určité riziká s externými stranami.

Znášanie rizík sa môže uskutočniť prostredníctvom poistenia, ktoré pokrýva následky, alebo prostredníctvom subdodávateľskej zmluvy s partnerom, ktorého úlohou je monitorovať informačný systém a prijať okamžité opatrenia.



Akceptácia rizika

Zvyškové je také **riziko**, ktorého hodnota po komplexnom ošetroaní rizík implementáciou pôvodných, dodatočných a rozšírených opatrení je taká nízka, že je pre organizáciu prijateľné a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie.



Vyhláška č. 227/2025 Z. z.

Súčasťou riadenia rizík je **analýza funkčného vplyvu (dopadov)**, ktorá pozostáva z hodnotenia vplyvu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy prevádzkovateľa základnej služby alebo spôsobiť ohrozenie alebo narušenie kontinuity jeho služieb. Súčasťou analýzy funkčného vplyvu je určenie cieľovej doby obnovy a cieľového bodu obnovy.



Analýza dopadov

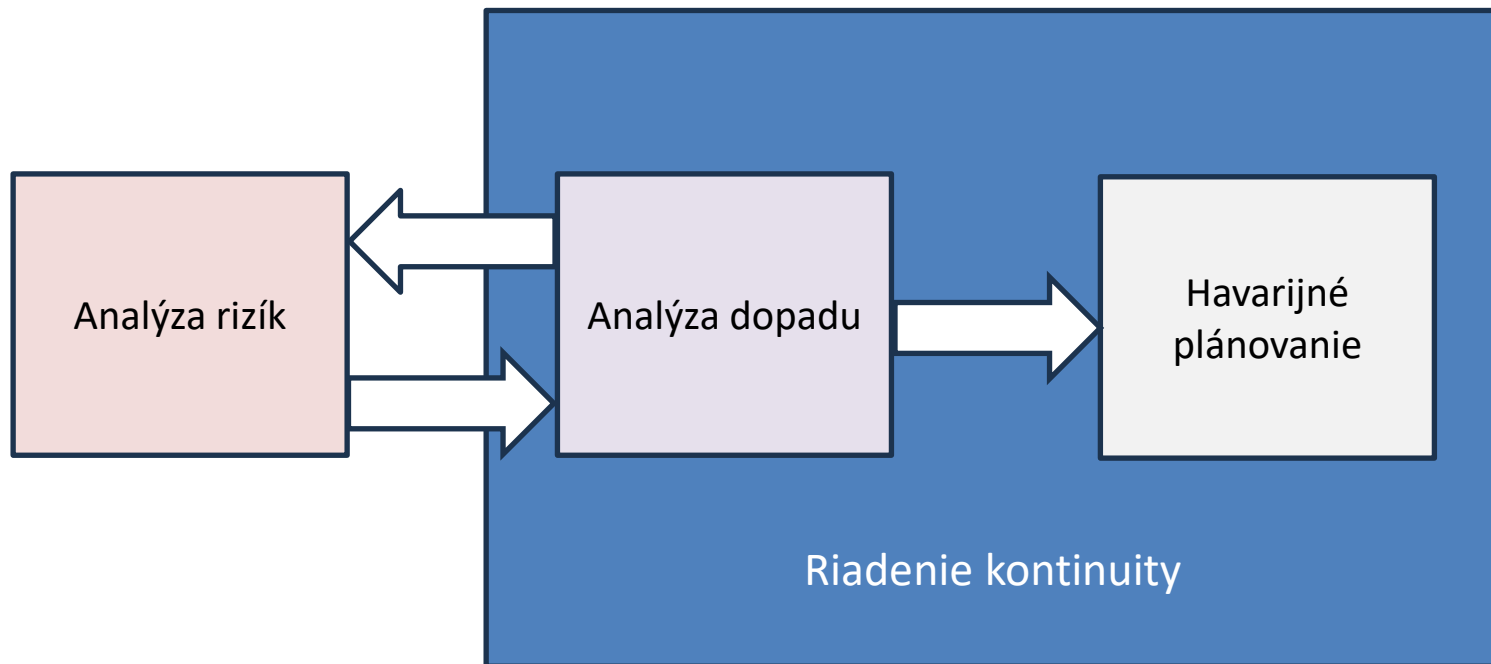
Analýzou dopadov sa identifikujú rôzne kategórie procesov organizácie, na základe ich kritickosti, ich vzájomnej závislosti, analyzujú sa potenciálne dôsledky (škôd/strát) pri rôznych dobách trvania kritických situácií, stanovujú sa maximálne akceptovateľné doby prerušenia (MTO), minimálne ciele kontinuity podnikania (MBCO), cieľové časy obnovy (RTO) a cieľové body obnovy (RPO).

Analýza dopadov je súčasťou procesu riadenia kontinuity činností, ktorý identifikuje potenciálne dopady vyplývajúce z možného prerušenia činností, a ktorého cieľom je pripraviť také postupy a vytvoriť také podmienky, ktoré zabezpečia v prípade krízovej situácie kontinuitu činností vo vopred stanovenom rozsahu a návrat k fungovaniu organizácie v normálnom režime.



Cieľom analýzy dopadov je najmä:

- zmapovanie procesov organizácie,
- identifikácia závislostí medzi procesmi,
- analýza možných dopadov a určenie MTO, MBCO, RTO a RPO,
- vymedzenie krízových situácií a eliminovanie ich dopadov,
- identifikáciu všetkých zdrojov a prostriedkov nevyhnutných na zabezpečenie kontinuity činností.





Kritické obdobie je obdobie v dni, týždni, mesiaci alebo roku, kedy je kontinuita procesu najkritickejšia, čiže proces je najcitlivejší a dopady v prípade kritickej situácie sú najvyššie. V prípade, že proces má stále rovnakú kritickosť na dopady, tak sa uvedie každý pracovný deň alebo každý kalendárny deň.

Množstvo práce, ktoré sa vykonáva v definovanom kritickom období znamená napríklad množstvo výrobkov alebo služieb, počet spracovaných položiek, transakcií a pod. za určitú jednotku času.

Množstvo práce, ktoré sa má vykonávať bezprostredne po krízovej situácii znamená napríklad množstvo výrobkov alebo služieb, počet spracovaných položiek, transakcií, atď. za určitú jednotku času. Je to minimálna úroveň služieb a/alebo produktov, ktorá je pre organizáciu prijateľná na dosiahnutie obchodných cieľov počas incidentu (MBCO).



Funkčným dopadom sa kvalitatívne hodnotí výška dopadu krízovej situácie v týchto oblastiach:

- strata reputácie,
- strata klientov / žiadateľov,
- dopad na iné činnosti organizácie,
- dopad na zdravie, bezpečnosť a prostredie.

Výška funkčného dopadu sa určuje zvlášť pre rôzne dĺžky trvania krízovej situácie. Rôzne dĺžky trvania krízovej situácie, pre ktoré sa budú hodnotiť dopady, budú definované na stretnutiach s vlastníkmi procesov.



Finančný dopad vyčísluje výšku priameho dopadu krízovej situácie v oblastiach:

- priame finančné škody,
- sankcie regulačných orgánov,
- zmluvné pokuty a/alebo uplatnenie náhrady škôd zo strany zmluvných partnerov,
- náklady súvisiace s návratom do normálneho stavu.

Výška finančného dopadu sa určuje zvlášť pre rôzne dĺžky trvania krízovej situácie. Rôzne dĺžky trvania krízovej situácie, pre ktoré sa budú hodnotiť dopady, budú definované na stretnutiach s vlastníkmi procesov. Samotná hodnota finančného dopadu sa určí sumou v EUR.



Stratu údajov kvalitatívne hodnotí výška dopadu straty údajov vyvolanou krízovou situáciou. Samostatne sa hodnotí maximálne množstvo údajov na základe hodnoty **RPO**, ktoré sa môžu stratiť v týchto formách:

- aplikácie, databázy,
- elektronické údaje, ktoré nie sú uložené v databázach (čiže napríklad údaje uložené na rôznych nosičoch ako CD, USB a pod.),
- papierové dokumenty.

Rôzne dopady sa posudzujú pre rôznu stratu údajov, podľa množstva údajov, ktoré sa vytvorili v poslednom časovom úseku. Jednotlivé časové úseky, pre ktoré sa budú hodnotiť dopady, budú definované na stretnutiach s vlastníkami procesov. Pre každú databázu, aplikáciu alebo informácie identifikované v analýze je potrebné vyhodnotiť maximálne množstvo údajov, ktoré sa môžu stratiť.



RPO - Recovery Point Objective

Vyjadrenie maximálne prijateľnej straty údajov, ktorá ešte nemá vysoké dopady na organizáciu. Tento parameter slúži ako požiadavka na zálohovací cyklus. Stupeň dopadu sa zvyčajne určuje v rozsahu do 2h, 4h, 8h, 24h, 48h, a 96h. Pre každý stupeň nedostupnosti je určená kritickosť výpadku v rozsahu 1 – 4. Posúdenie dopadu:

- (1)** - Okrajový
- (2)** - Akceptovateľný
- (3)** - Vysoký
- (4)** - Kritický

Ako hranica akceptovateľnosti je hodnota " 1 – 2 ", Stupeň "3" predstavuje dopad zo straty údajov za vysoký. Táto hodnota sa definuje ako hraničná a dĺžka straty údajov vyjadrená v čase. Strata údajov "3" sa definuje ako požiadavka na minimálny zálohovací cyklus.



RPO - Recovery Point Objective

- **Strata údajov:** Ak organizácia nedosiahne stanovený RPO, môže dôjsť k strate dôležitých údajov. To môže mať vážne následky, najmä ak ide o citlivé alebo kritické informácie. Strata údajov môže mať negatívny vplyv na efektivitu, kontinuitu a bezpečnosť činnosti organizácie.
- **Obnovenie údajov:** Ak je RPO prekročené, obnovenie údajov môže byť zložitejšie a náročnejšie. Organizácia sa môže stretnúť s výzvami pri obnove nedostatkových alebo poškodených údajov. To môže spomaliť proces obnovy a predĺžiť čas obnovenia prevádzky.



Identifikácia zdrojov a prostriedkov na obnovu procesu sa bude vykonávať iba pre procesy, ktoré majú zásadný vplyv na kontinuitu činností organizácie. Tieto procesy budú identifikované v rámci analýzy, na základe ich hodnoty **RTO**. Je potrebné identifikovať tieto typy zdrojov:

- ľudia,
- aplikácie / databázy,
- údaje uložené v elektronickej podobe (nezahrnuté v aplikáciách a databázach),
- údaje uložené na papierovom médiu,
- IT a komunikačné zariadenia,
- komunikačné kanály,
- ostatné vybavenie,
- vybavenie a infraštruktúra,
- pracovný kapitál.

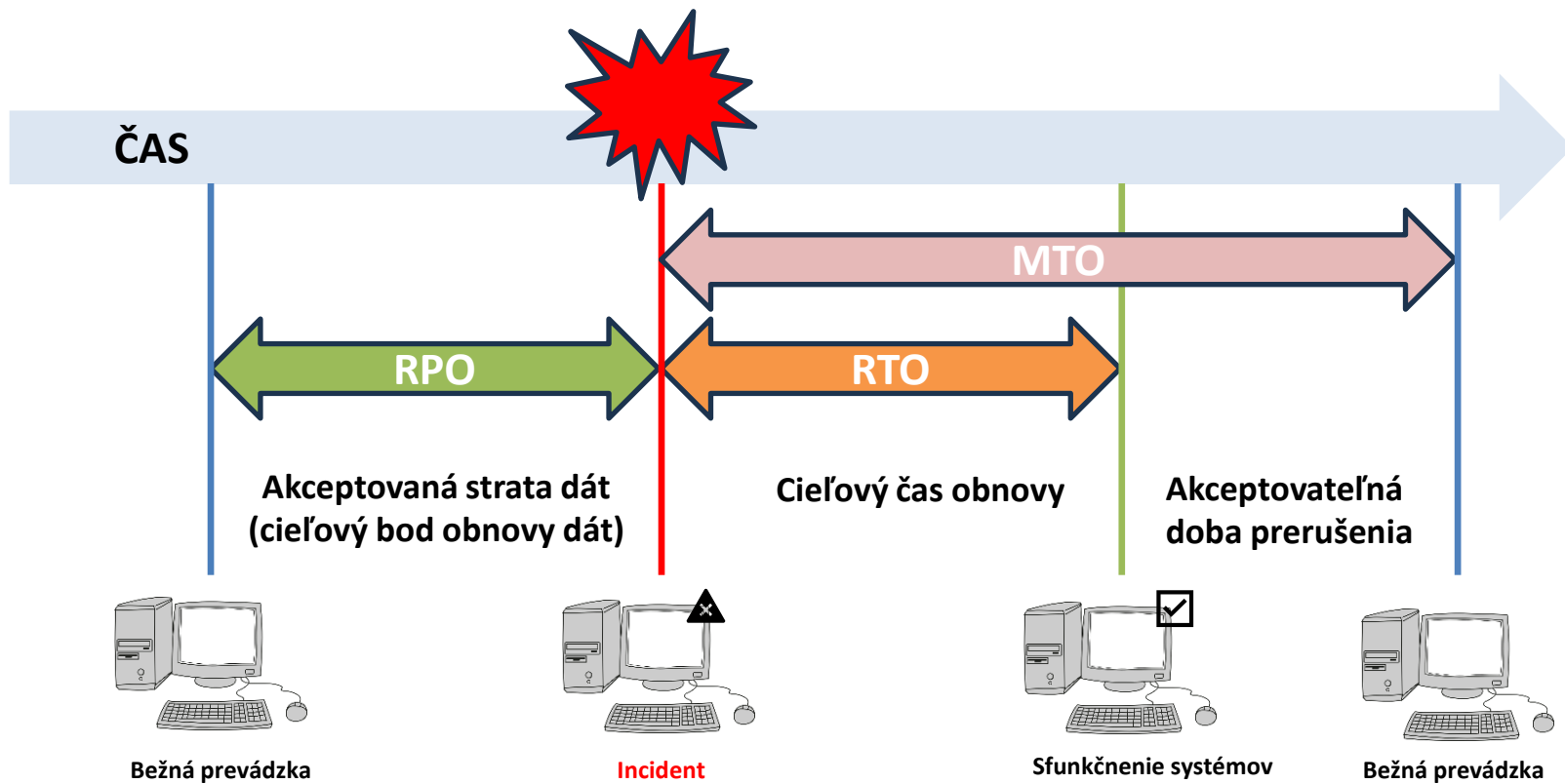


RTO - Recovery Time Objective

Označuje čas, do ktorého treba obnoviť funkčnosť kritických procesov po ich prerušení. Stupeň dopadu sa zvyčajne určuje v rozsahu do 2h, 4h, 8h, 24h, 48h, a 96h. Pre každý stupeň nedostupnosti je určená kritickosť výpadku v rozsahu 1 – 4. Posúdenie dopadu:

- (1) - Okrajový
- (2) - Akceptovateľný
- (3) - Vysoký
- (4) - Kritický

Ako hranica akceptovateľnosti je hodnota " 1 - 2 ", Stupeň "3" predstavuje dopad vysoký. Táto hodnota sa definuje ako hraničná dĺžka nedostupnosti a definuje sa ako SLA dostupnosť pre daný proces. RTO pre informačné systémy, aplikácie a databázy sa určí ako minimálne RTO všetkých procesov, ktoré sú závislé na danom informačnom systéme, aplikácii a databáze.





Ďakujem za pozornosť

V prípade záujmu navštívte našu stránku www.somi.sk alebo FB <https://www.facebook.com/somi.sk>
E-mailový kontakt: daniel.schikor@somisk.sk