10.9 Řízení kontinuity činností

Tento dokument popisuje opatření, která MUSÍ, nebo BY MĚLA být implementována pro

- **Práva a povinnosti zúčastněných osob.**
- **Cíle řízení kontinuity činností**
- **Naplnění cílů kontinuity činností.**
- **Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.**
- **Určení a obsah potřebných plánů kontinuity a havarijních plánů.**
- **Pravidla a postupy pro realizaci opatření.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Systém řízení bezpečnosti informací (§ 15).

1. Práva a povinnosti zúčastněných osob

Cíl: Cílem je stanovit práva a povinnosti administrátorů a osob zastávajících bezpečnostní role formou „Kdo, kdy, a co má v průběhu mimořádné situace dělat“ (např. eskalační postupy).

1.1 Práva

Opatření: Organizace MUSÍ stanovit práva zúčastněných osob v řízení kontinuity činností – jedná se o výkonný management a řídící pracovní skupinu odpovědnou za řízení kontinuity činností.

1.2 Povinnosti

Opatření: Organizace MUSÍ stanovit povinnosti zúčastněných osob v řízení kontinuity činností. Cílem kontinuity provozních činností je poskytnout výkonnému vedení jistotu, že kritické procesy (ať už automatizované či nikoliv) budou v krizových situacích nadále fungovat na přijatelné úrovni prostřednictvím toho, že se budou soustředit na udržování dostupnosti kritických informací a infrastruktury. Organizace MUSÍ začlenit odpovědnosti do organizační struktury a do procesů v organizaci.

2 Cíle řízení kontinuity činností

Cíl: Stanovení rozsahu a hranic řízení kontinuity činností. Pomocí hodnocení rizik a analýzy dopadů organizace vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika související s ohrožením kontinuity činností.

Plán kontinuity činnosti MUSÍ zahrnovat:

- reakci na incidenty
- obnovu po havárii
- krizová řízení

Řízení kontinuity činností se MUSÍ stát součástí procesů v organizaci a být realizováno na základě modelu PDCA (viz Příloha B).

2.1 Minimální úroveň poskytovaných služeb (MBCO)

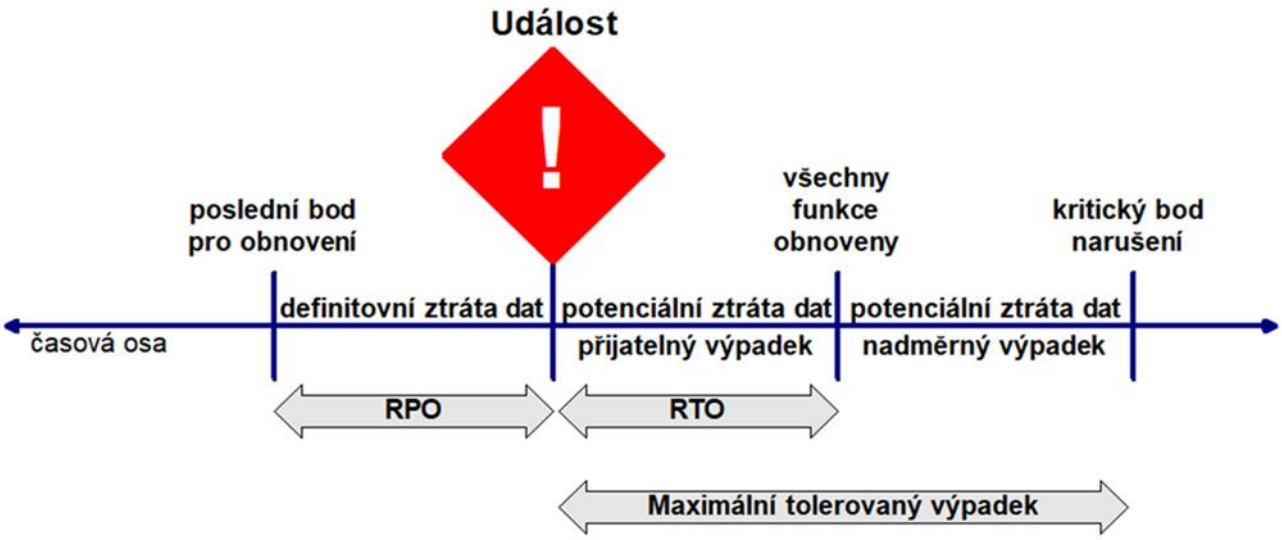
Opatření: Organizace MUSÍ stanovit minimální úroveň poskytovaných služeb. MBCO znamená minimální úroveň služeb nebo produktů, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému.

2.2 Doba obnovení chodu (RTO)

Opatření: Organizace MUSÍ stanovit dobu obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému

2.3 Bod obnovení dat (RPO)

Opatření: Organizace MUSÍ stanovit bod obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.



Obr. 1 Cíl obnovy ve vztahu k události

3 Naplnění cílů kontinuity činností

Cíl: Organizace MUSÍ vytvořit postupy, které budou obsahovat naplnění cílů podle předchozího bodu. Tzn., jakým způsobem organizace dosáhne toho, aby udržela minimální akceptovatelnou úroveň služeb. Organizace MUSÍ vytvořit postupy, havarijní plány, DRP pro obnovu chodu informačního nebo komunikačního systému, na základě výše uvedených cílů.

3.1 Přiřazení adekvátních zdrojů

Opatření: Organizace MUSÍ přiřadit adekvátní lidské a materiální zdroje.

Implementační pokyny:

3.1.1 Nutnost posouzení investice do řízení kontinuity činností vůči alternativním nákladům (ušlé zisky, pokuty, neschopnost získávat nové smlouvy, ztráta zákazníků).

3.2 Časový rámec

Opatření: Organizace BY MĚLA zajistit dostatek času pro implementaci řízení kontinuity činnosti.

Implementační pokyny:

3.2.1 Vytvoření času a prostoru pro implementační tým z pohledu školení o implementaci, jednotlivých úkolů při aktivaci plánu a samotné implementace ve formě jednotlivých plánů.

3.3 Školení a oprávnění implementačního týmu

Opatření: Organizace MUSÍ zabezpečit zdroje pro budování povědomí o řízení kontinuity činností.

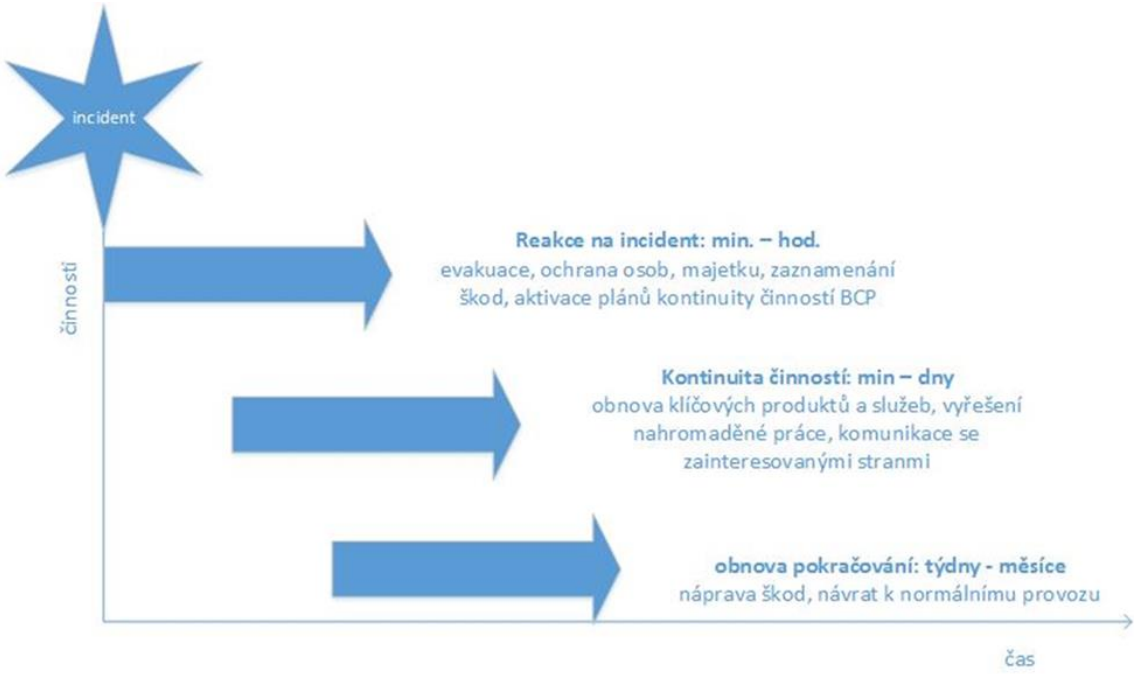
Implementační pokyny:

3.3.1 Organizace MUSÍ zajistit, aby se v organizaci vědělo, že vůbec BCM je zavedena a proč.

3.3.2 Jakmile existují plány, je nutné zajistit, aby to všichni věděli a věděli jaká je jejich úloha při aktivaci plánů poručená dokumentace.

4 Způsoby hodnocení dopadů incidentů na kontinuitu a hodnocení rizik

Cíl: Identifikace potenciálních dopadů incidentů a stanovení strategického a provozního rámce k aktivnímu zvyšování odolnosti organizace proti přerušení, narušení výroby, nebo ztrátě služeb.



Obr. 2 Časový přehled reakce na incident

4.1 Analýza dopadů

Opatření: Organizace BY MĚLA nastavit pravidla pro analýzu dopadů (BIA – Business Impact Analysis).

Implementační pokyny:

4.1.1 BIA je činnost identifikující kritické činnosti, které umožňují organizaci plnit jejich cíle (dodávat služby, produkty). BIA je orientována na dopad, nikoli na příčinu.

4.1.2 Organizace MUSÍ zvážit, jaký by byl dopad na ni samotnou a další zainteresované strany, kdyby byly dodávky klíčových produktů nebo služeb a jejich podpůrné kritické činnosti z jakéhokoliv důvodu narušeny.

4.2 Analýza rizik

Opatření: Organizace MUSÍ provést analýzu rizik ve vztahu ke zdrojům, které byly identifikovány při mapování procesů a posléze jim přiřazeny. Identifikovaná rizika je nutné snižovat a řídit.

Implementační pokyny:

4.2.1 Organizace MUSÍ identifikovat **SPoF** (Single Point of Failure) z pohledu:

- klíčových pracovníků
- klíčových dodavatelů
- specifických technologií

atd.

5 Určení a obsah potřebných plánů kontinuity a havarijních plánů

Cíl: Organizace MUSÍ zabezpečit řádné naplánování řízení kontinuity činností s plnou podporou vrcholového vedení.

5.1 Obsah plánu

Opatření: Organizace MUSÍ zajistit metodiku plánování řízení kontinuity činností.

Implementační pokyny:

5.1.1 Plán kontinuity činností MUSÍ BÝT kontinuální, dokumentovaný, rozvíjený a implementovaný do procesů organizace.

5.1.2 Plán kontinuity vychází z identifikace požadavků řízení kontinuity činností, stanovení cílů a rozsahu.

5.1.3 Plán kontinuity činností poskytuje odpovědi na základní otázky:

- co se má udělat
- kdy
- kde jsou umístěny alternativní zdroje
- kdo je zapojen
- jak se má dosáhnout kontinuity činností

5.1.4 Plány MUSÍ BÝT verzovány a jejich verze řízeny.

5.1.5 Plány MUSÍ BÝT přístupné v době krize.

5.1.6 Obsah plánů řízení kontinuity činností:

- účel a rozsah
- role a odpovědnosti
- aktivace plánu
- alternativní lokality
- plány obnovy systému (DRP – Disaster Recovery Plan)
- kontaktní údaje
- priority
- důležité dokumenty a zdroje
- kontrolní seznamy
- lidé
- veřejný profil
- záchranné operace
- návrat k normálu.

5.1.7 Plány MUSÍ BÝT po vytvoření implementovány.

5.1.8 Plány MUSÍ BÝT testovány a procvičovány na základě schváleného scénáře a výsledky MUSÍ BÝT přezkoumány a vyhodnoceny včetně zpracování zprávy o testování.

5.2 Plánu obnovy po havárii

Opatření: Organizace MUSÍ zajistit optimalizaci plánu po havárii (DR plan).

Implementační pokyny:

- Plán obnovy po havárii IT musí mít přesný seznam komunikace.
- Scénář obnovy musí být podrobný, srozumitelný, přesný a jasný.
- Opětovné testování plánu obnovy IT po havárii.
- Všichni členové týmu plánu obnovy by měli znát své role.
- Plán obnovy musí obsahovat seznam zdrojů přístupných 24 hodin na místě obnovy.
- Plán obnovy musí obsahovat seznam aplikací do plánu po havárii.
- Plán obnovy by měl obsahovat aktuální schéma sítě v místě obnovy.
- Plán obnovy by měl obsahovat aktuální přístupovou mapu a pokyny, jak dosáhnout místa obnovy.
- Měla by být poskytnuta další dokumentace (seznam kontaktů dodavatelů, pojištění, HW a SW aktiv.
- Plán obnovy musí být udržován v aktuálním stavu.

6 Pravidla a postupy pro realizaci opatření

Cíl: Organizace realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům a omezení dostupnosti.

6.1 Přijatá opatření

Opatření: Výsledkem přezkoumání je zpráva, kde bude uvedeno, jaká mají být přijata opatření, kdo je za implementaci zodpovědný, a kdy mají být opatření implementována.

Implementační pokyny:

6.1.1 Opatření typu **náprava** – eliminace příčin neshod a přijatá nápravná opatření.

6.1.2 **Preventivní opatření** – identifikace, určení a zavedení preventivních opatření včetně stanovení priorit. Preventivní opatření musí být přiměřená dopadu.

6.1.3 Hodnocení rizik a stav plánu zvládání rizik.

6.1.4 Identifikace možností pro neustálé zlepšování.

6.1.5 Doporučení potřebných rozhodnutí, stanovení opatření a odpovědných osob.

6.1.6 **Opatření pro zajišťování úrovně dostupnosti** informačního a komunikačního systému, důležitých technických aktiv informačního a komunikačního systému.

6.1.7 **Opatření pro zajišťování redundance** aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

Použité zdroje

(1) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

(2) *MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD* [online]. Verze 1.0. NÚKIB, 2020 [cit. 2022-04-20]. Dostupné z: https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)

Příloha B: Řízení kontinuity činností podle PDCA modelu