10.14 Zálohování a obnova a dlouhodobé ukládání

Tento dokument popisuje opatření, které MUSÍ nebo BY MĚLO být implementováno pro:

- **Požadavky na zálohování a obnovu.**
- **Pravidla a postupy zálohování.**
- **Pravidla a postupy dlouhodobého ukládání (archivace).**
- **Pravidla bezpečného zálohování a archivace dat.**
- **Pravidla a postupy obnovy.**
- **Pravidla a postupy testování zálohování a obnovy.**
- **Pravidla přístupu k zálohám a ukládaným informacím.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti (VKB) – Řízení provozu a komunikací (VKB § 10).

1 Požadavky na zálohování a obnovu

1.1 Pravidla a postupy zálohování a dlouhodobého ukládání (archivace)

Cíl: Zajistit správný a bezpečný proces řízení záloh a dlouhodobě uložených dat.

Společnost MUSÍ stanovit pravidla pro zálohování a archivaci dat.

Implementační pokyny:

1.1.1 Návrh informačního nebo komunikačního systému MUSÍ obsahovat požadavky na zálohování, které vychází ze SLA (Service-level agreement) parametrů informačního nebo komunikačního systému (tedy dostupnosti).

1.1.2 Plán ochrany dat MUSÍ být vypracován před nasazením do rutinního provozu:

- Proces zálohování MUSÍ být jasně definovaný a dokumentovaný
- Ke každému zálohovacímu procesu MUSÍ být určen garant, který je zodpovědný za vytváření a následnou kontrolu použitelnosti zálohy pro obnovu

1.1.2 MUSÍ být stanoveny zásady garantujících kompletnost, dostupnost a 100% obnovu ze zálohy:

- Pro každé aktivum BY MĚLA být stanovena hodnota RPO (Recovery Point Objective, cílový bod obnovy)
- Pro každé aktivum BY MĚLA být stanovena hodnota RTO (Recovery Time Objective, cílová doba obnovy)
- Definice parametrů RPO a RTO viz Příloha B.

1.1.3 MUSÍ být zohledněno pravidlo maximální dostupnosti dat

- Zohlednění MUSÍ být postaveno na klíčových parametrech pro stanovení dostupnosti MTBF (střední doba mezi poruchami) a MTTR (střední doba potřebná k opravě).

1.1.4 MĚLO BY platit pravidlo 3-2-1 pro zálohování dat

- Doporučením je propracovaný systém zálohování ve formátu 3-2-1 (3 kopie na 2 typech médií a jednu zálohu mimo vlastní sítě, nejlépe u umístění informačního nebo komunikačního systému („offsite“).

1.1.5 MĚL BY být zohledněn relevantní požadavek na šifrování zálohovaných dat viz bod 1.2.1 Klasifikace a kategorizace dat.

1.2 Rozsah použití

MUSÍ být nastaven rozsah použití záloh a archivace zohledňujícím dopad na provoz.

Implementační pokyny:

1.2.1 Data BY MĚLA být klasifikována a kategorizována na (viz Příloha C):

- Data společná, data specifická.
- Data určená k zálohování, data určená k archivaci.

1.2.2 Za klasifikaci a kategorizaci dat MUSÍ být odpovědný garant aktiva.

1.2.3 MUSÍ být zálohována specifická provozní a bezpečnostní data:

- Data týkající se zranitelností aktiv (CVE, VU, ICSA).
- Data související s patch managementem zařízení a aplikací.
- Bezpečnostní data z výstupu logování.

1.2.4 Mimořádné zálohy MUSÍ být prováděny na základě provozní potřeby.

1.2.5 Archivace dat se řídí „Archivačním a skartačním řádem“.

2 Pravidla a postupy testování zálohování a obnovy

Společnost MUSÍ provádět pravidelné zálohování a pravidelně kontrolovat použitelnost provedených záloh.

Implementační pokyny:

2.1.1 Čitelnosti záloh a archívu MUSÍ být kontrolována:

- Za stanovení postupu je odpovědný garant aktiva.
- MĚL BY být stanoven harmonogram pro kontrolu čitelnosti záloh a archívu.
- Všechny kontroly čitelnosti záloh a archívu MUSÍ být zdokumentovány.

2.1.2 Zálohy a archívy MUSÍ být testovány:

- Za stanovení postupu je odpovědný garant aktiva.
- MĚL BY být stanoven harmonogram pro testování záloh a archívu.
- Všechny kontroly testování záloh a archívu MUSÍ být zdokumentovány.

2.1.3 MUSÍ být vytvořen detailního návrh zálohování celého informačního nebo komunikačního systému.

2.1.4 Popis BY MĚL mít strukturu, viz Tabulka 1.

Tabulka 1: Ukázka popisu nastavení zálohování

Server	Co zálohovat	Interval	Kolik záloh uchovávat	Kolik dní uchovávat zálohy	Jak často provádět rozdílové zálohy	Kdy probíhá zálohování	Předpokládaná doba obnovy
Server-x	Celý server	týdně	30	730	denně	18:00-18:10	30 minut

3 Pravidla bezpečného zálohování a dlouhodobého ukládání informací

Společnost MUSÍ stanovit a dodržovat pravidla pro bezpečné zálohování a archivaci dat.

Implementační pokyny:

3.1.1 Zálohovaná a archivovaná data BY MĚLA být zašifrována.

3.1.2 MĚLY BY být stanoveny bezpečnostní prvky pro jednotlivé kategorie (viz Příloha D).

3.1.3 Uložiště dat MUSÍ být zabezpečena:

- Řešení zabezpečení zařízení a médií včetně jejich správy BY MĚLO vycházet z normy ČSN EN ISO/IEC 27040:2017.

3.2 RACI matice zálohování a archivace dat

Společnost MUSÍ definovat role a odpovědnosti ve vztahu k zálohování a archivaci dat, nejlépe formou matice rolí a odpovědností.

Implementační pokyny:

3.2.1 Činnosti dle obecné tabulky MUSÍ společnost přesně definovat, nejlépe podle algoritmů zálohování a archivace.

3.2.2 Společnost MUSÍ zajistit informovanost dotčených subjektů o obsahu RACI matice.

Tabulka 2: Obecný vzor RACI matice:

	Role A	Role B	Role C
Činnost 1	Typ odpovědnosti	Typ odpovědnosti	Typ odpovědnosti
Činnost 2	Typ odpovědnosti	Typ odpovědnosti	Typ odpovědnosti
Činnost 3	Typ odpovědnosti	Typ odpovědnosti	Typ odpovědnosti

3.3 Algoritmus zálohování (viz Příloha E)

Společnost BY MĚLA implementovat algoritmus pro zálohování.

Implementační pokyny:

3.3.1 Společnost BY MĚLA pověřit odpovědnou osobu (Manažera kybernetické bezpečnosti, MKB) vytvořením algoritmu zálohování.

3.3.2 Společnost BY MĚLA zajistit implementaci algoritmu zálohování a jeho následné aktualizace (v případě potřeby).

3.3.3 Po implementaci algoritmu pro zálohování společnosti MUSÍ vymáhat jeho dodržování.

3.4 Algoritmus archivace (viz Příloha F)

Společnost BY MĚLA implementovat algoritmus pro archivaci.

Implementační pokyny:

3.4.1 Společnost BY MĚLA pověřit odpovědnou osobu (MKB) vytvořením algoritmu zálohování.

3.4.2 Společnost BY MĚLA zajistit implementaci algoritmu archivace a jeho následné aktualizace (v případě potřeby).

3.4.3 Po implementaci algoritmu pro archivaci společnosti MUSÍ vymáhat jeho dodržování.

4 Pravidla a postupy obnovy

Společnost MUSÍ stanovit pravidla a postupy obnovení dat po havárii (incidentu).

4.1.1 MUSÍ být vytvořen Disaster Recovery plan:

- MUSÍ být stanoveny scénáře pro případ částečných a absolutních výpadků, dále viz směrnice SM-23 Řízení kontinuity činností.

Použité zdroje

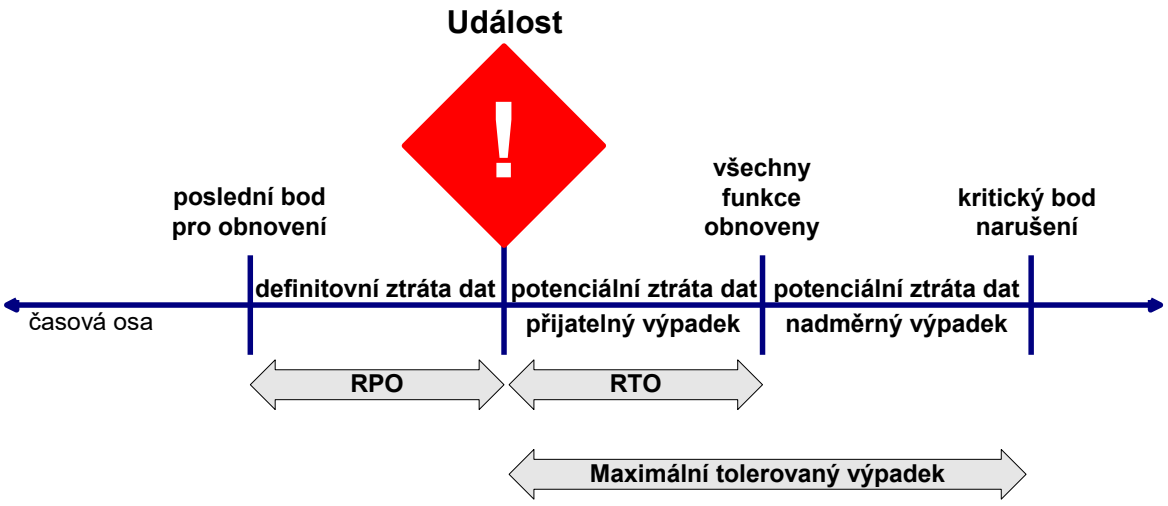
(1) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, 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: Definice parametrů RPO a RTO



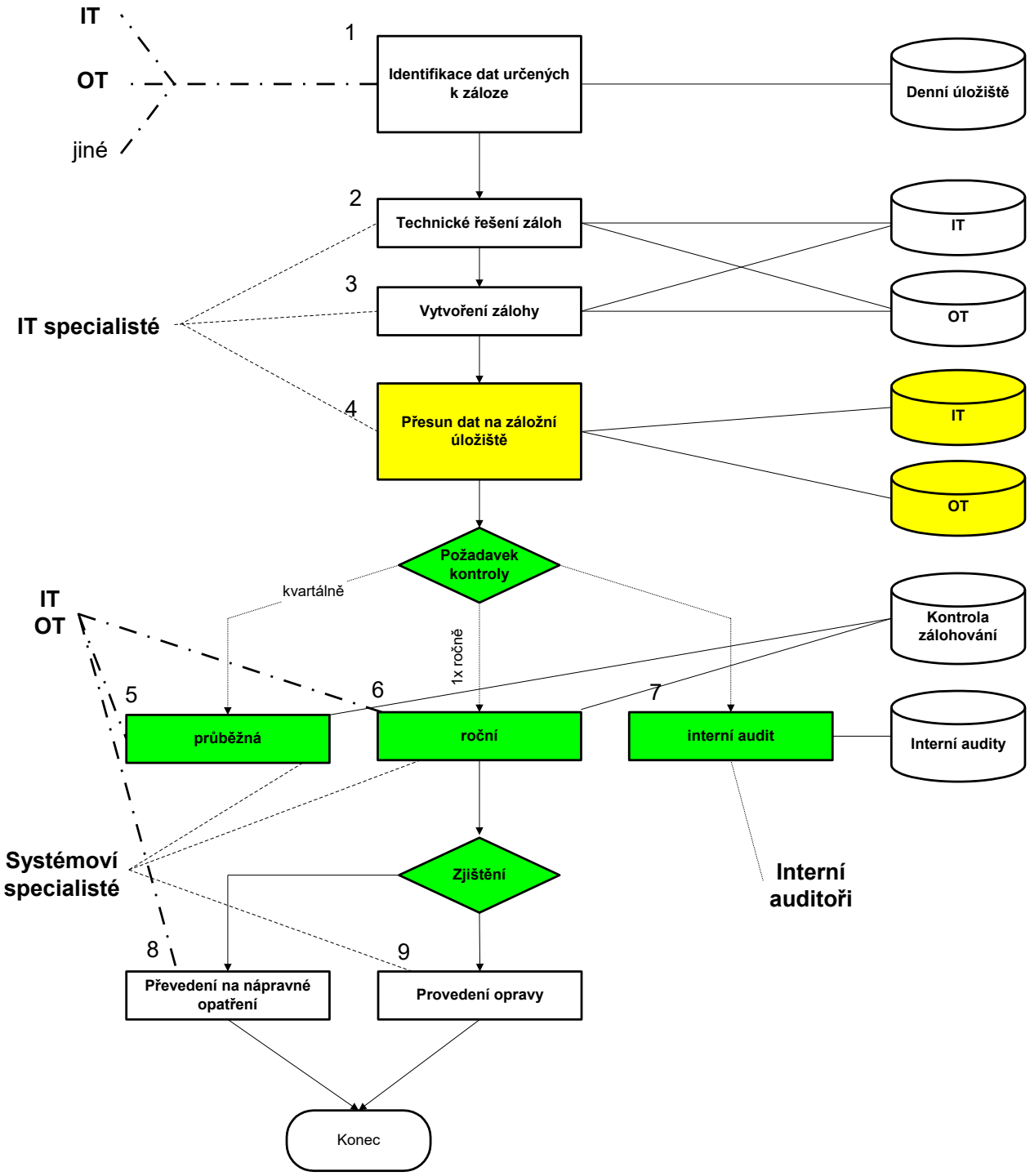
Příloha C: Příklad kategorizace informací

Úroveň		Označení	Popis kategorie
1	Minimum	VEŘEJNÉ (S0)	Informace určené pro zaměstnance a partnery (informace z webu, novinové články).
2	Standard	INTERNÍ (S1)	Vnitropodniková dokumentace dostupná všem zaměstnancům (směrnice, firemní předpisy).
3	Nadstandard	CITLIVÉ (DŮVĚRNÉ) (S2)	Informace důležité pro chod firmy (smlouvy, osobní údaje).
4	Kritické	TAJNÉ (KRITICKÉ) (S3)	Strategické firemní informace (strategické projekty).

Příloha D: Příklad bezpečnostních prvků

Opatření	Interní informace (S1)	Důvěrné informace (S2)	Tajné informace (S3)
Povinnost označení dokumentu	Není	Na prvním listě	Na prvním listě + vodotisk
Evidence počtu stran	Není	Označení počtu stran na prvním listě	Označení počtu stran na všech stranách dokumentu
Předání dokumentu třetí straně	Bez omezení	Musí existovat smlouva o mlčenlivosti, souhlas vlastníka dokumentu	Musí existovat smlouva o mlčenlivosti, souhlas vlastníka dokumentu a člena vedení firmy, záznam o předání
Přenášení dokumentů el. poštou – interně	Bez omezení	Omezit na nezbytné příjemce, bez další ochrany	Přenos dokumentů chráněn heslem, které je předáno jinou formou
Přenášení dokumentů el. poštou – externě	Bez omezení	Omezit na nezbytné příjemce, je-li žádoucí pak aplikovat ochranu heslem	Nepřípustné
Uložení na souborovém systému	Bez omezení	Pouze do určených složek, kde je omezený přístup	Dokumenty mohou být uloženy pouze lokálně
Revize přístupových oprávnění	1x ročně	1x za pololetí	1x čtvrtletně
Ukládání dokumentů na mobilní počítače	Bez omezení	Pouze na nezbytně nutnou dobu a uživatel musí zajistit ochranu mobilního počítače před zcizením nebo zneužitím	Pouze v šifrované podobě a uživatel musí zajistit ochranu mobilního počítače před zcizením nebo zneužitím
Ukládání na výměnná média	Bez omezení	Pouze na nezbytně nutnou dobu a uživatel musí zajistit ochranu výměnného média	Pouze v šifrované podobě

Příloha E: Algoritmus zálohování



Příloha F: Algoritmus archivace