10.12 Řízení změn

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

- **Způsob a principy řízení významných změn.**
- **Přezkoumávání dopadů významných změn.**
- **Způsob vedení evidence a testování významných změn.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Řízení změn (§ 11).

1 Způsob a principy řízení významných změn

Cíl: Identifikování změn, které jsou podstatné z hlediska kybernetické bezpečnosti a mohou ji pozitivně nebo negativně ovlivnit. Nastavení postupů pro řízení změn tak, aby se minimalizovala možnost narušení správné funkčnosti daného informačního nebo komunikačního systému (případně bezpečnosti informací).

1.1 Určení významné změny

Společnost MUSÍ určit významné změny, například pomocí argumentu změn.

Implementační pokyny:

1.1.1 Příklady argumentu změny jsou uvedeny v Tabulce 1.

Tabulka 1: Argument změny

ID	Kritérium
1	Změna v rámci jednoho primárního aktiva/systému
2	Změna s dopadem na dva a více primárních aktiv /systémů
3	Změna vyvolaná dodavatelem/provozovatelem systému
4	Změna ve společné infrastruktuře
5	Organizační změny s dopadem na primární aktivum
6	Legislativní změny
7	Definované provozní změny

1.1 Řízení změn podle argumentu změny

MUSÍ být nastaveny adekvátní postupy, které by neměly za následek negativní dopad na provoz.

Implementační pokyny:

1.1.2 Změna v rámci jednoho primárního aktiva/systému:

- Za stanovení postupu je odpovědný garant aktiva.
- Při posuzování dopadu změny MUSÍ být zvažována všechna podpůrná aktiva.

1.1.3 Změna s dopadem na dva a více primárních aktiv /systémů:

- Za stanovení postupu je odpovědný garant aktiva, které je dotčeno iniciačním požadavkem na změnu.
- MĚLA BY být ustavena komunikační matice a způsob komunikace zúčastněných stran.
- Při posuzování dopadu změny MUSÍ být zvažována všechna podpůrná aktiva.

1.1.4 Změna vyvolaná dodavatelem/provozovatelem systému:

- Za stanovení postupu je odpovědný garant aktiva dotčeného iniciačním požadavkem na změnu.
- MĚLA BY být ustavena komunikační matice, a způsob komunikace zúčastněných stran.
- Při posuzování dopadu změny MUSÍ být zvažovány všechny podpůrná aktiva.
- Při posuzování dopadu změny MUSÍ být zvažovány i smluvní podmínky dodavatele/provozovatele.

1.1.5 Změna ve společné infrastruktuře:

- Za stanovení postupu je odpovědný útvar.
- Při posuzování dopadu změny MUSÍ být zvažovány vazby na relevantní podpůrná aktiva.

1.1.6 Definované provozní změny:

- Jedná se o kategorii změn nastavených v rámci standardních odsouhlasených procedur bez nutnosti vypracování speciálního postupu.

2 Přezkum dopadů významných změn

Přezkoumání a následné seznámení uživatelů s možnými dopady změn. Uživatelé MUSÍ být seznámeni s možnými dopady změn, společnost BY MĚLA vhodnou formou vysvětlit výsledky přezkoumání možných dopadů změn.

Implementační pokyny:

2.1.1 Společnost MUSÍ přezkoumat dle přesně stanovených postupů možné dopady změn. Viz příloha B

2.1.2 Uživatelé MUSÍ sdílet odpovídající povědomí o možných dopadech změn.

2.1.3 Společnost MUSÍ zajistit informovanost uživatelů o možných dopadech změn. Uživatelé BY MĚLI být informování definovanou formou o možném dopadu změn. Viz příloha B

3 Způsob vedení evidence a testování významných změn

Společnost MUSÍ vést dokumentaci řízení změn, aktualizovat a zpřístupnit informace pro provedení změny. Společnost stanoví pravidla pro testování a případnou možnost návratu do původního stavu.

Implementační pokyny:

3.1.1 Postupy pro řízení změn související se zařízeními pro zpracování informací a komunikací MUSÍ být zdokumentovány.

3.1.2 Provozní postupy a zdokumentované postupy pro změny v systémech BY MĚLY podléhat formální správě dokumentů a změny BY MĚLY být schváleny zodpovědným vedoucím.

3.1.3 Dokumentace procesu změny BY MĚLA přesně určit následující aspekty (pokud to je relevantní):

a) Změny v systémech a zařízeních zařazených do primárních aktiv
b) Změny v ostatních systémech a zařízeních
c) Změny v síťové infrastruktuře
d) Změny HW a SW
e) Změny procesů a pracovních postupů
f) Organizační změny
g) Změny notifikační a publikační

3.1.4 Dokumentace procesu změny BY MĚLA obsahovat analýzu rizik (pokud to je relevantní)

3.1.5 Na základě výsledků analýzy rizik BY MĚLO být rozhodnuto o provedení penetračních testů nebo testování zranitelnosti.

3.1.6 Společnost, pokud na základě analýzy rizik rozhodne, MUSÍ provádět penetrační testy informačního a komunikačního systému se zaměřením na důležitá aktiva před jejich uvedením do provozu a v souvislosti s významnou změnou a MUSÍ reagovat na zjištěné nedostatky. Více viz metodika NÚKIB – PENETRAČNÍ TESTOVÁNÍ (1).

3.1.7 Dokumentace procesu změny BY MĚLA obsahovat aktualizaci bezpečnostní politiky a bezpečnostní dokumentace (pokud to je relevantní).

3.1.8 Proces návratu do původního stavu (Exit strategie) BY MĚLA být součástí směrnice SM-6 Řízení provozu a komunikací.

3 Řízení změn služeb dodavatelů

3.1.9 Řízení dodavatelů, odstavec 4.2

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

(3) *PENETRAČNÍ TESTOVÁNÍ – ÚVOD DO PROBLEMATIKY NÚKIB* [online]. Brno: NÚKIB, 2022 [cit. 2022-05-01]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/2022-03-07_Penetracni-testovani_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: Formulář pro dokumentaci a oznámení změn

	Útvar	**E-mailová adresa:**	
		Telefonní číslo:	
OZNÁMENÍ ZMĚN			
…..			
Aktivum/systém:		Garant aktiva/předkladatel požadavku na změnu	Datum zaslání
ID změny			
Verze oznamované změny			
Název změny			
Stručný popis změny			
Předpokládané dopady změny na aktivum			
Termín plánovaného zavedení (dd.mm.rrrr)			
Kontaktní pracovník (email, tel. spojení)			
Změna schvalovaná (A/N)			
Doplňující informace (volitelné)	*Např. předpokládané dopad změny na služby, jaká se předpokládají dočasná omezení, školení apod.*		
(Poznámka)			