GUARDIANS CZ

Srovnání změn bezpečnostních požadavků pro vyšší režim regulace

Pracovní verze ke dni 18.5.2025

Upozornění:
Nejedná se o oficiální materiál, ale o pomůcku pro rychlý přehled o některých změnách.

Oblast	**Popis změn**
Předmět úpravy (§ 1)	Odstranění úpravy nezbytného rozsahu strategicky významné služby z této vyhlášky, vč. Přílohy č. 8 - Rozsah strategicky významných služeb. **Bude upraveno nařízením vlády.**
Vymezení pojmů (§ 2)	Přidání konkrétního odkazu na paragraf (§ 12 odst. 1 písm. a)), kde jsou stanovena pravidla pro určení významných změn. Mírná formulační změna u definice významného dodavatele (významný dodavatel poskytuje plnění významné pro kybernetickou bezpečnost).
Systém řízení bezpečnosti informací (§ 4)	Rozšíření a zpřesnění kritérií pro vyhodnocení účinnosti a následnou aktualizaci systému řízení bezpečnosti informací. Zohledňuje se 7 kritérií - výsledky předchozího hodnocení, posouzení dopadů incidentů na oblast kybernetické bezpečnosti, posouzení významných změn podle § 12.
Požadavky na vrcholné vedení (§ 5)	Explicitní požadavek na školení pro všechny členy vrcholného vedení s odkazem na konkrétní paragraf školení (§ 11 odst. 3 písm. a)). Podrobněji rozepisuje povinnosti vrcholného vedení vůči výboru (schválení zřízení, zajištění složení, jednání, záznamy, způsobilosti členů). Přidání požadavku na vymezení práv a povinností při určování osob do bezp. rolí.

Řízení bezpečnostní politiky a dokumentace (§ 7)	V § 7 byl odstraněn explicitní požadavek na stanovení pravidel pro protiopatření a explicitní požadavek na určení odpovědné osoby za přezkum/aktualizaci dokumentace.
Řízení aktiv (§ 8)	Explicitní požadavek na stanovení metodik pro určování a hodnocení aktiv. Zavedení požadavku na evidenci garantů aktiv. Zjednodušení výčtu konkrétních bodů, které musí pravidla ochrany aktiv obsahovat (např. nezmiňuje explicitně pravidla pro značení, výměnná média, sdílení, likvidaci v tomto bodě).
Příloha č. 1 - Hodnocení aktiv	Explicitní odkaz na stanovení metodiky v § 8. Přidání sloupce s příklady pravidel ochrany aktiva do tabulek hodnocení úrovní.
Řízení rizik (§ 9)	Výrazné rozšíření seznamu faktorů, které musí být zohledněny při hodnocení rizik (hrozby, zranitelnosti, dopady na aktiva, významné změny, změny stanoveného rozsahu, protiopatření, incidenty, audity/kontroly, výsledky testování/skenování, vyhodnocení účinnosti ISMS). Metody zvládání rizik jsou přesunuty z přílohy přímo do hlavního textu paragrafu.
Řízení dodavatelů (§ 10)	Zkrácení a zjednodušení seznamu náležitostí, které musí obsahovat písemné vyrozumění významného dodavatele o jeho evidenci (odebrán požadavek na uvedení obsahu pravidel pro dodavatele).
Bezpečnost lidských zdrojů (§ 11)	Přidání explicitního požadavku na zahrnutí potřebných teoretických i praktických školení do plánu rozvoje bezpečnostního povědomí (poučení vedení, poučení uživatelů/admin./bezp.rolí, potřebná teoretická i praktická školení). Pravidla tvorby hesel jsou explicitně odkázána na § 20.
Řízení změn (§ 12)	Upřesnění požadavku, že určování významných změn musí být v souladu se stanovenými kritérii. Změna odkazu na konkrétní odstavec v § 25 pro penetrační testování (odst. 5 místo odst. 6).

Akvizice, vývoj a údržba (§ 13)	Přidání požadavku, aby bezpečnostní požadavky pro akvizici, vývoj a údržbu zohledňovaly relevantní bezpečnostní opatření z této vyhlášky.
Řízení přístupu (§ 14)	U požadavku na řízení přístupu byla odstraněna fráze "na základě bezpečnostních a provozních potřeb". Přidání explicitního požadavku na oddělení uživatelských a administrátorských účtů pro jednu osobu. Konkrétnější odkaz na paragraf (§ 21), kde je popsán nástroj pro řízení přístupových práv.
Zvládání kybernetických bezpečnostních událostí a incidentů (§ 15)	**Doplněn požadavek na vytvoření závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu s významným dopadem podle § 16 zákona, včetně popisu příčiny vzniku kybernetické bezpečnostního incidentu s významným dopadem, pokud je známa.**
Provádění auditu kybernetické bezpečnosti (§ 17)	Odstranění požadavku na posuzování souladu s "jinými předpisy" při auditu. Změna odkazu na odstavec pro dříve stanovená nápravná opatření (§17(2)(c)). Zjednodušení seznamu, kam se zohledňují výsledky auditu (vypuštěno "plán zvládání rizik" a "prohlášení o aplikovatelnosti", zobecněno na "v rámci řízení rizik").
Řízení identit a autentizace (§ 20)	Zavedení explicitních minimálních délek hesel pro různé typy účtů při standardní autentizaci (12 znaků pro uživatele, 17 pro administrátory, 22 pro technická aktiva (při použití hesla/jména)). Přidání specifických, přísnějších pravidel pro administrátorské účty, zejména pro účely obnovy (vynucení změny výchozího hesla, použití náhodného řetězce).
Zaznamenávání událostí (§ 23)	Upřesnění, že aktualizace rozsahu logovaných aktiv probíhá pravidelně a při významných změnách. Zpřesnění, že mezi zaznamenávané detaily patří i jednoznačná identifikace technického aktiva, které událost zaznamenalo, i při změně síťové identifikace.

Penetrační testování (§ 25)	Změna odkazu z §12(3) na §25 (odst. 5 místo odst. 6).

Pozn.: Zpracováno na základě porovnání původní teze vyhlášky a návrhu vyhlášky publikované 16.5.2025 v MPŘ, s podporou nástroje NotebookLM.