Financováno Evropskou unií
NextGenerationEU

NÁRODNÍ PLÁN OBNOVY

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

podpůrný materiál 4.2-1

Řízení rizik správy dat

verze 1.0

vytvořeno v rámci projektu

Zajištění podmínek pro kvalitní správu datového fondu a zajištění řízeného přístupu k datům

Reg.č.: CZ.31.1.01/MV/23_62/000006

Obsah

1 Úvod

Metodika stanovuje jednotný rámec pro identifikaci, popis, hodnocení a prioritizaci rizik správy dat v organizacích veřejné správy. Je určena pro odborné role odpovědné za správu dat, řízení rizik a kybernetickou bezpečnost.

Metodika vychází ze struktury a popisu oblastí správy dat ve veřejné správě, navazuje na „Strategii řízeného přístupu k datům pro zajištění podmínek pro kvalitní správu datového fondu VS ČR“ a na procesy řízení rizik organizace.

Klíčovým prvkem metodiky je „Katalog hrozeb a rizik správy dat“ (dále uváděn jako „Katalog“), který je koncipován jako analytický nástroj vycházející z uvedených zdrojů a slouží k podpoře zajištění trvalého zvyšování odolnosti organizace vůči dopadům nezvládnuté správy dat.

Účelem Katalogu je vytvořit jednotný a stabilní referenční rámec pro systematickou identifikaci, popis a řízení rizik spojených s daty jako s aktivem organizace.

Katalog umožňuje pracovat s riziky správy dat dlouhodobě, opakovatelně a konzistentně napříč organizačními útvary, datovými oblastmi i časem.

Základním východiskem Katalogu jsou typové kritické faktory správy dat, které reprezentují témata správy dat, jejichž pokrytí je nezbytné pro řádné fungování práce s daty. Rizika správy dat jsou v Katalogu chápána jako důsledky selhání nebo nedostatečného pokrytí těchto témat, nikoli jako izolované problémy nebo incidenty.

Katalog není určen k evidenci jednotlivých incidentů, problémů nebo projektových zjištění. Jeho cílem je zachytit typické a opakující se způsoby selhání správy dat, jejich příčiny a možné dopady na fungování organizace, a vytvořit tak stabilní základ pro řízení rizik.

Katalog zejména:

- převádí obecné problémy v oblasti dat do strukturovaně popsaných rizik,
- podporuje jednotné chápání rizik správy dat napříč organizací,
- poskytuje podklad pro jejich prioritizaci na základě dopadů,
- vytváří vazbu mezi identifikací rizik a řízením opatření.

Katalog se zaměřuje výhradně na rizika vznikající v oblasti správy dat, zejména v souvislosti s obsahem, významem, kvalitou, dostupností a využitelností dat.

2 Základní principy Katalogu

2.1 Co je riziko správy dat

Riziko správy dat je možnost, že v důsledku nedostatků ve správě dat (např. nejasné odpovědnosti, nízké kvality, nedostatečné ochrany nebo chybného řízení změn) dojde k negativním dopadům na činnost organizace. Riziko je v metodice chápáno jako kombinace hrozby, zranitelnosti a dopadu; pro účely prioritizace se klade důraz zejména na závažnost dopadu.

Obecně je riziko vyjádřením nejistoty ve vztahu k cílům organizace. V praxi řízení rizik se rizika evidují, hodnotí a řídí prostřednictvím opatření tak, aby se snížila pravděpodobnost nebo dopad nežádoucích událostí.

V kybernetické bezpečnosti se riziko typicky vztahuje k ohrožení aktiv prostřednictvím kybernetických hrozeb a zranitelností. Rizika správy dat s kybernetickou bezpečností úzce souvisejí: slabá správa dat představuje vnitřní zranitelnost, která může zvyšovat pravděpodobnost i dopady kybernetických incidentů, a současně může vést k významným dopadům i bez přítomnosti kybernetického útoku.

2.2 Princip kauzality

Katalog je založen na kauzálním pojetí rizik. Riziko není chápáno jako izolovaný problém nebo incident, ale jako výsledek kauzálního řetězce: klíčový faktor → kritický faktor (příčina) → zranitelnost → hrozba → riziko → dopad. Každý prvek má v Katalogu samostatnou roli a je navázán na typové seznamy.

Tento přístup umožňuje oddělit příčiny rizik od jejich projevů, identifikovat systémová selhání správy dat a cílit řízení rizik na oblasti, kde lze dosáhnout největšího efektu.

2.3 Odlišení od kybernetických incidentů

Katalog se zaměřuje výhradně na rizika vznikající v oblasti správy dat, zejména v souvislosti s jejich obsahem, významem, kvalitou, dostupností a využitelností.

Neřeší technické bezpečnostní incidenty, útoky ani kompromitaci informačních systémů.

Toto oddělení umožňuje zachovat jasné vymezení odpovědností mezi správou dat a kybernetickou bezpečností, zabránit duplicitnímu popisu rizik a současně vytvořit prostor pro eskalaci rizik správy dat do rámce řízení rizik kybernetické bezpečnosti v případech, kdy jejich dopady ohrožují regulované služby nebo aktiva.

2.4 Důraz na dopad

Prioritizace rizik je primárně dopadově orientovaná. Smyslem Katalogu je zachytit rizika s významnými dopady na výkon organizace a její zákonné/strategické povinnosti i v situacích, kdy pravděpodobnost nelze spolehlivě kvantifikovat.

2.5 Typovost strukturálních prvků

Katalog je navržen jako typový z hlediska struktury a příčin rizik, nikoli jako nahodilý výčet izolovaných situací. Typovost zajišťuje srovnatelnost, sdílení poznatků napříč organizacemi a možnost postupné standardizace.

Konkrétní rizika představují aplikaci těchto typových prvků na specifický kontext organizace, datové oblasti nebo procesu. Tento přístup umožňuje zachovat konkrétnost rizik a zároveň zajistit jejich srovnatelnost, opakovatelnost a systematičnost.

2.6 Podpora cílených a účinných opatření

Struktura Katalogu je navržena tak, aby podporovala cílení opatření na skutečné příčiny rizik, nikoli pouze na jejich projevy.

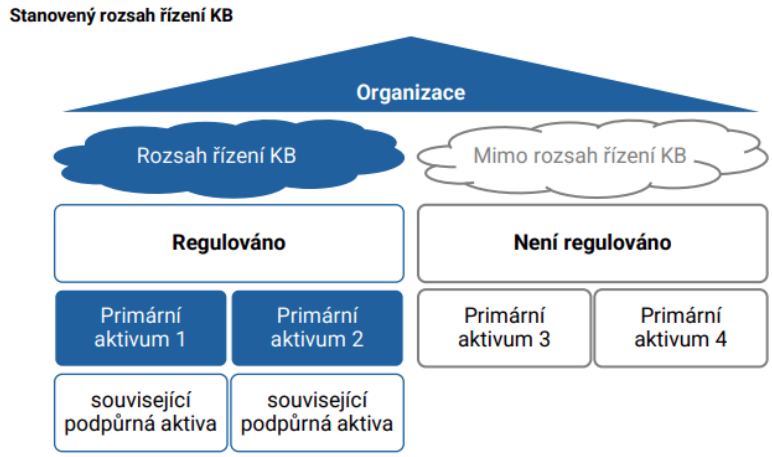
Členění kritických faktorů pod le jejich charakteru (organizační, procesní, právní a regulatorní, kulturní, bezpečnostní, ekonomický a technický) umožňuje navrhovat opatření s jasným adresátem odpovědnosti a zvyšovat jejich účinnost a udržitelnost.

2.7 Integrace s řízením rizik organizace

Správa dat a kybernetická bezpečnost představují dvě vzájemně provázané, avšak významově odlišné oblasti řízení organizace. Kybernetická bezpečnost se v souladu s regulatorním rámcem zaměřuje na vymezený okruh regulovaných služeb, informačních systémů a datových aktiv. Naproti tomu správa dat se vztahuje na veškerá data organizace, bez ohledu na to, zda jsou součástí regulované služby nebo nikoli.

Tento rozdíl v rozsahu působnosti je klíčový pro pochopení role „Katalogu hrozeb a rizik správy dat“. Katalog umožňuje systematicky identifikovat a popisovat rizika vyplývající z nedostatečné správy dat v celém datovém prostoru organizace, včetně oblastí, které nejsou přímo pokryty režimem kybernetické bezpečnosti.

Integrovaný přístup ke správě dat a kybernetické bezpečnosti vytváří prostor pro využití existujících procesů řízení rizik, kontrol a přezkumu i pro rizika správy dat. Správa dat přináší obsahové porozumění významu dat, jejich vazbám na agendy organizace a dopadům jejich selhání, zatímco kybernetická bezpečnost poskytuje procesní rámec pro jejich systematické řízení.



Zdroj: NÚKIB, podpůrný materiál „Stanovení rozsahu řízení kybernetické bezpečnosti“, 24.10.2025

Obrázek znázorňuje vztah obou oblastí: kybernetická bezpečnost pokrývá vymezenou podmnožinu datových aktiv organizace, zatímco správa dat se vztahuje na celý datový prostor. Tento vztah umožňuje identifikovat rizika správy dat, která mají potenciál eskalovat do oblasti kybernetické bezpečnosti v případech, kdy jejich dopady ohrožují regulované služby nebo klíčová aktiva-

Katalog je navržen tak, aby byl kompatibilní s existujícími procesy řízení rizik. Umožňuje převést záznamy do interní evidence rizik organizace a napojit je na rozhodování o opatřeních, prioritách a investicích.

3 Struktura katalogu

3.1 Struktura záznamu rizika

Katalog je koncipován jako hierarchicky členěná evidence. Pracuje s typovými strukturálními prvky, které umožňují jednotný popis napříč agendami a organizacemi.

Každý záznam v Katalogu je strukturován tak, aby umožňoval srozumitelný, kauzálně konzistentní a opakovatelný popis rizika včetně jeho příčin, projevů a dopadů.

Záznam rizika je jednotný datový objekt, který propojuje příčiny a dopady v rámci kauzálního řetězce. Minimální struktura záznamu zahrnuje: identifikaci rizika, popis kauzálního řetězce (kritický faktor → zranitelnost → hrozba → riziko → dopad), přiřazené typové položky, odpovědnosti a navržená preventivní a reaktivní opatření.

3.2 Typové seznamy

Katalog je postaven na sadě typových seznamů, které tvoří jeho metodický a obsahový základ. Typové seznamy nepopisují konkrétní situace v jednotlivých organizacích, ale zachycují obecné a opakující se vzorce selhání správy dat, které se mohou v různých kontextech projevovat odlišným způsobem. Konkrétní rizika v Katalogu pak vznikají kombinací typových prvků s konkrétním kontextem organizace, datové oblasti nebo procesu.

Typové seznamy plní v Katalogu několik klíčových funkcí:

- vytvářejí jednotný a sdílený jazyk pro popis rizik správy dat,
- zajišťují srovnatelnost rizik napříč datovými oblastmi a organizacemi,
- podporují opakovatelnou práci s riziky v čase,
- a vytvářejí přímou vazbu mezi identifikací rizik a řízením opatření.

Charakteristika jednotlivých typových seznamů:

Typové kritické faktory správy dat

- Představují základní příčiny selhání správy dat. Popisují oblasti, ve kterých nedostatečné nastavení, chybějící procesy, nejasné odpovědnosti nebo nedostatečné kompetence vedou ke vzniku rizik.
- Kritické faktory jsou členěny podle svého charakteru (organizační, procesní, právní a regulatorní, kulturní, bezpečnostní, ekonomický a technický), což umožňuje identifikovat skutečné kořenové příčiny rizik a cílit řízení rizik i návrh opatření na odpovídající úroveň řízení.

Typové příčiny správy dat

- Představují konkrétní mechanismy selhání, které vznikají v důsledku nenaplněných kritických faktorů správy dat. Zachycují bezprostřední důvody vzniku problémů, například chybné postupy, nejednoznačné interpretace pravidel nebo nedostatečnou koordinaci činností.

Typové zranitelnosti správy dat

- Popisují stav správy dat, který umožňuje uplatnění hrozby. Vycházejí z kombinace typových kritických faktorů a konkrétního kontextu organizace.

Typové hrozby působící na data

- Popisují způsob, jakým se zranitelnosti správy dat mohou projevit v reálném fungování organizace. Nejde o bezpečnostní útoky ani technické incidenty, ale o situace, ve kterých se slabiny správy dat projeví negativním dopadem.

Typové rizika správy dat

- Slouží k zachycení typických rizik, která vznikají kombinací zranitelností a působících hrozeb v oblasti správy dat.
- Nejsou popisem konkrétní události v organizaci, ale obecně formulovanými rizikovými scénáři, které se mohou opakovat napříč různými organizacemi a kontexty.

Typové dopady správy dat

- Popisují následky selhání správy dat na fungování organizace, plnění agend, rozhodování, důvěryhodnost a vztahy s okolím.

- Typové dopady nejsou odvozeny z pravděpodobnosti výskytu, ale z povahy a významu následků.
- Typové dopady slouží jako společný referenční rámec pro hodnocení a prioritizaci rizik správy dat a umožňují jejich srozumitelnou komunikaci napříč organizací.

4 Prioritizace rizik správy dat

Prioritizace rizik správy dat je navržena tak, aby byla kompatibilní s řízením rizik kybernetické bezpečnosti, nikoli aby jej nahrazovala nebo duplikovala. Rizika správy dat jsou posuzována z hlediska jejich obsahových a organizačních dopadů, zatímco kybernetická bezpečnost se zaměřuje na hrozby a incidenty v oblasti ochrany aktiv.

Prioritizace rizik správy dat představuje klíčový krok, který umožňuje převést analytický popis rizik do roviny rozhodování a řízení. Jejím cílem není detailní kvantifikace rizik, ale určení relativní významnosti rizik správy dat v konkrétním organizačním kontextu.

4.1 Princip dopadově orientované prioritizace

Prioritizace rizik správy dat vychází z posouzení dopadů možného selhání správy dat na fungování organizace. Není primárně založena na odhadu pravděpodobnosti, ale na významu a závažnosti následků, které mohou nastat.

Tento přístup odpovídá povaze rizik správy dat, jejichž dopady jsou často zřejmé a opakovaně pozorovatelné, zatímco pravděpodobnost jejich vzniku je silně závislá na konkrétním kontextu a obtížně kvantifikovatelná.

4.2 Hodnocená hlediska (kritéria)

Hodnocení dopadu je založeno na posouzení dopadu z několika vzájemně se doplňujících hledisek (kritérií). Tato kritéria představují doporučený referenční rámec, který organizacím pomáhá uvažovat o dopadech rizik správy dat systematicky a konzistentně. Organizace mohou kritéria upravit, rozšířit nebo zjednodušit dle svého rámce řízení rizik.

K1 – Rozsah dopadu

- Kritérium posuzuje, jak velké části organizace se dopad rizika týká

K2 – Závažnost dopadu na fungování a rozhodování

- Kritérium posuzuje, jak závažné následky má realizace rizika na schopnost organizace fungovat a rozhodovat

K3 – Náročnost nápravy a obnovy

- Kritérium posuzuje, jak obtížné je odstranit následky realizovaného rizika a obnovit správný stav.

K4 – Reputační, právní a strategické dopady

- Kritérium posuzuje dopady, které přesahují bezprostřední provozní rovinu.

4.3 Výstup prioritizace

Výstupem prioritizace je určení relativní priority rizika na základě hodnocení dopadu:

- kritická priorita,

- vysoká priorita,
- střední priorita,
- nízká priorita.

Priorita je využita pro plánování opatření, alokaci zdrojů a řízení změn. U rizik s vysokým dopadem se přednostně uplatňují preventivní opatření a průběžný monitoring.

4.4 Vazba na opatření

Ke každému riziku se přiřazují preventivní a reaktivní opatření. Opatření se volí cíleně podle místa zásahu v kauzálním řetězci (odstranění příčiny, snížení zranitelnosti, omezení dopadu). Zvolená opatření musí být dohledatelně přiřazena k odpovědné roli a k procesu řízení změn.

5 Integrace a scénáře použití

5.1 Integrace do řízení rizik

Katalog je určen k napojení na stávající systém řízení rizik organizace. Záznamy z Katalogu mohou být převáděny do interní evidence rizik včetně přiřazení vlastníků, priorit, opatření a termínů. Metodika podporuje pravidelný přezkum rizik, sledování trendů a řízení změn.

5.2 Integrace do kybernetické bezpečnosti

Rizika správy dat jsou z pohledu kybernetické bezpečnosti vnitřní zranitelností organizace: zvyšují pravděpodobnost i dopady kybernetických incidentů a současně mohou způsobit významné dopady i bez útoku. Integrace s kybernetickou bezpečností proto zahrnuje zejména: (a) vazbu na primární aktivum „Data“, (b) propojení zranitelností správy dat s kybernetickými scénáři/incidenty, (c) společné využití dopadových kategorií pro hodnocení významnosti a (d) koordinaci preventivních a reaktivních opatření.

5.3 Scénáře použití katalogu

Katalog je určen pro využití zejména v těchto situacích:

- průběžné řízení rizik správy dat,
- řešení incidentu nebo problému s daty,
- posuzování změn informačních systémů a datových toků,
- audit a hodnocení souladu v oblasti kybernetické bezpečnosti,
- plánování preventivních opatření a zvyšování odolnosti organizace.

5.3.1 Scénář 1: Použití Katalogu v rámci pravidelného řízení rizik organizace

Výchozí situace

Organizace provádí pravidelné řízení rizik v rámci existujících procesů, včetně řízení rizik kybernetické bezpečnosti. Rizika související s daty jsou dosud posuzována převážně z technického nebo systémového pohledu.

Použití Katalogu

Katalog je využit jako referenční rámec pro identifikaci a strukturování rizik vyplývajících z nedostatečné správy dat, jejich významu, kvality, dostupnosti a využitelnosti. Katalog umožňuje tato rizika systematicky zohlednit v rámci stávajících procesů řízení rizik organizace.

Výstupy a návaznosti

Identifikovaná rizika správy dat jsou posouzena z hlediska jejich dopadů na fungování organizace a slouží jako podklad pro jejich prioritizaci. V případech, kdy mají významné dopady nebo vazbu na regulované služby, jsou eskalována do oblasti řízení rizik kybernetické bezpečnosti. Výstupem je integrovaný pohled na rizika správy dat v rámci celkového rizikového profilu organizace.

5.3.2 Scénář 2: Použití Katalogu při řešení konkrétního problému nebo incidentu souvisejícího s daty

Výchozí situace

V organizaci dojde ke konkrétnímu problému nebo incidentu souvisejícímu s daty, například k významné chybě v datech, jejich nesprávné interpretaci, omezené dostupnosti, nekonzistenci nebo k narušení důvěryhodnosti dat využívaných pro rozhodování nebo plnění agend. Problém může mít provozní, organizační nebo reputační dopady, aniž by nutně šlo o kybernetický bezpečnostní incident.

Použití Katalogu

Katalog je v tomto scénáři využit jako analytický nástroj pro strukturované pochopení příčin vzniklého problému. Umožňuje zasadit konkrétní incident do širšího kontextu správy dat a identifikovat kritické faktory a zranitelnosti, které k jeho vzniku vedly.

Prostřednictvím Katalogu je možné odlišit bezprostřední projev problému od jeho systémových příčin v oblasti správy dat, například v nastavení odpovědností, procesech řízení kvality dat, významu dat nebo jejich využívání. Katalog tak podporuje posun od reaktivního řešení jednotlivého problému k pochopení opakovatelných vzorců selhání.

Výstupy a návaznosti

Výstupem scénáře je strukturovaný popis rizik správy dat souvisejících s řešeným problémem, včetně identifikace jejich příčin a možných dopadů. Tyto informace slouží jako podklad pro rozhodnutí o nápravných a preventivních opatřeních v oblasti správy dat.

V případech, kdy řešený problém nebo identifikovaná rizika správy dat mají významné dopady na regulované služby nebo klíčová aktiva, mohou být výsledky analýzy využity jako vstup do řízení rizik kybernetické bezpečnosti. Scénář tím podporuje koordinaci řešení problémů v oblasti dat a kybernetické bezpečnosti bez směšování jejich odpovědností.

5.3.3 Scénář 3: Použití Katalogu při změně informačního systému, datového toku nebo významné změně dat

Výchozí situace

Organizace připravuje nebo realizuje změnu informačního systému, datového toku nebo významnou změnu dat, například migraci dat, změnu zdrojového systému, úpravu integračních vazeb, změnu struktury dat nebo změnu jejich významu v souvislosti s úpravou agendy. Tyto změny jsou zpravidla posuzovány z hlediska technické realizovatelnosti, nákladů a harmonogramu, zatímco dopady na správu dat a jejich využití nemusí být systematicky zohledněny.

Použití Katalogu

Katalog je v tomto scénáři využit jako analytický rámec pro posouzení dopadů plánované změny na data a jejich využití v organizaci. Umožňuje identifikovat rizika spojená se změnou významu dat, jejich kvality, konzistence, dostupnosti a návaznosti na další datové oblasti a procesy.

Pomocí Katalogu lze strukturovaně posoudit, zda plánovaná změna nevytváří nové zranitelnosti správy dat nebo nezvyšuje rizika v oblastech, které jsou klíčové pro plnění agend nebo rozhodování. Katalog slouží jako referenční rámec pro odbornou diskusi mezi IT, vlastníky dat a dalšími dotčenými rolemi, aniž by nahrazoval projektové nebo technické řízení změny.

Výstupy a návaznosti

Výstupem scénáře je identifikace a popis rizik správy dat vyvolaných plánovanou nebo realizovanou změnou, včetně jejich možných dopadů na fungování organizace. Tyto informace slouží jako podklad pro rozhodnutí o úpravách návrhu změny, doplnění opatření v oblasti správy dat nebo o změně způsobu realizace.

V případech, kdy identifikovaná rizika správy dat mají významné dopady na regulované služby, klíčová aktiva nebo bezpečnostní cíle organizace, mohou být výsledky analýzy využity jako vstup do řízení rizik kybernetické bezpečnosti. Scénář tím podporuje koordinované řízení změn v oblasti IT, dat a kybernetické bezpečnosti.

5.3.4 Scénář 4: Využití Katalogu v rámci auditu a přezkumu řízení kybernetické bezpečnosti

Výchozí situace

Organizace provádí audit nebo pravidelný přezkum řízení kybernetické bezpečnosti, ať už v rámci interních kontrolních mechanismů, externího auditu nebo plnění regulatorních požadavků. Pozornost auditu je zpravidla zaměřena na technická a procesní opatření, zatímco rizika vyplývající z nedostatečné správy dat nemusí být zachycena v plném rozsahu.

Použití Katalogu

Katalog je v tomto scénáři využit jako doplněk k existujícímu rámci auditu a přezkumu řízení kybernetické bezpečnosti. Umožňuje identifikovat rizika správy dat, která mají významné dopady na fungování organizace, ale nejsou vždy zachycena prostřednictvím technicky orientovaných kontrol.

Katalog slouží jako referenční rámec pro posouzení, zda jsou v organizaci systematicky řešeny příčiny rizik souvisejících s významem dat, jejich kvalitou, dostupností a využitelností, a zda jsou tato rizika adekvátně integrována do řízení rizik kybernetické bezpečnosti.

Výstupy a návaznosti

Výstupem scénáře je rozšířený pohled na rizika organizace, který propojuje výsledky auditu kybernetické bezpečnosti s riziky správy dat. Identifikovaná rizika správy dat mohou být využita jako podklad pro úpravu závěrů auditu, návrh nápravných opatření nebo zpřesnění rizikového profilu organizace.

V případech, kdy audit nebo přezkum identifikuje významné nedostatky v oblasti správy dat s dopady na regulované služby nebo klíčová aktiva, mohou být tato zjištění eskalována do řízení rizik kybernetické bezpečnosti. Scénář tím podporuje konzistentní propojení auditu, řízení rizik a správy dat bez vytváření paralelních kontrolních struktur.

5.3.5 Scénář 5: Použití Katalogu pro řízení opatření a prevenci rizik v oblasti správy dat

Výchozí situace

Organizace se systematicky věnuje správě dat a usiluje o předcházení rizikům, která mohou vznikat v důsledku nedostatečně nastavených procesů, odpovědností nebo pravidel správy dat. V rámci řízení rizik již identifikovala rizika správy dat, avšak potřebuje lépe propojit jejich řízení s plánováním a vyhodnocováním preventivních opatření.

Použití Katalogu

Katalog je v tomto scénáři využit jako referenční rámec pro strukturování preventivních opatření v oblasti správy dat. Umožňuje vazbu mezi identifikovanými riziky správy dat, jejich příčinami a zranitelnostmi a opatřeními, která mají za cíl tato rizika snižovat nebo jim předcházet.

Katalog podporuje systematický pohled na prevenci rizik správy dat tím, že pomáhá identifikovat oblasti, ve kterých je vhodné posílit procesy správy dat, vyjasnit odpovědnosti, upravit pravidla nebo zlepšit práci s daty, aniž by bylo nutné zavádět samostatný systém řízení opatření.

Výstupy a návaznosti

Výstupem scénáře je přehled preventivních opatření v oblasti správy dat, která jsou navázána na identifikovaná rizika a jejich příčiny. Tento přehled slouží jako podklad pro plánování, realizaci a vyhodnocování opatření v oblasti správy dat a pro sledování jejich účinnosti.

V případech, kdy preventivní opatření v oblasti správy dat přispívají ke snížení rizik s dopady na regulované služby nebo klíčová aktiva, mohou být jejich výsledky zohledněny také v rámci řízení rizik kybernetické bezpečnosti. Scénář tím podporuje dlouhodobé a koordinované snižování rizik napříč oblastmi správy dat a kybernetické bezpečnosti.

5.4 Jak číst a používat uvedené scénáře

Uvedené scénáře nejsou normativním popisem povinného workflow. Pouze ukazují, jak lze Katalog využít například při pravidelném řízení rizik, při řešení incidentů, při změnách informačních systémů a datových toků, při auditech a přezkumech nebo při komunikaci s vedením organizace. Jsou záměrně formulovány tak, aby respektovaly rozdílnou úroveň zralosti správy dat v organizacích a umožňovaly postupné a přiměřené zapojení Katalogu do řízení rizik organizace. Nevyžadují budování paralelních procesů a jsou navrženy takovým způsobem, aby byly maximálně kompatibilní s existujícími mechanismy řízení rizik, zejména v oblasti kybernetické bezpečnosti.

Jejich cílem je usnadnit praktickou aplikaci metodiky a ukázat, že Katalog není teoretickým artefaktem, ale je a může být nástrojem každodenní řídicí praxe.

6 Role a provoz

6.1 Role a odpovědnosti

Řízení rizik správy dat vyžaduje jasné přiřazení odpovědností.

Klíčové role v oblasti správy dat:

- datový architekt plní roli vlastníka Katalogu rizik správy dat (správce metodiky a typových seznamů) a zajišťuje koordinaci s řízením rizik a kybernetickou bezpečností
- vlastníci a věcní správci dat jsou garanty domén/datových oblastí a zajištění věcnou správnost prioritizace rizik a smysluplné řízení opatření (plánování a realizace)
- garant správy dat rozhoduje o prioritách v oblasti řízení rizik správy dat

Role v oblasti řízení rizik a kybernetické bezpečnosti:

- manažer kybernetické bezpečnosti
- manažer řízení rizik (pokud je role oddělena)

Role vedení organizace

Konkrétní role mohou být v organizaci sloučeny, musí však být zachována odpovědnost za rozhodování a dohledatelnost.

6.2 Spolupráce rolí v praxi

Řízení rizik správy dat je založeno na spolupráci více rolí, nikoli na izolované odpovědnosti jednotlivců.

Typicky platí, že:

- vlastníci dat poskytují obsahový a významový kontext,
- správci dat a datoví architekti zajišťují systematičnost,
- manažeři kybernetické bezpečnosti a řízení rizik propojují rizika do širšího rámce,
- garant správy dat, případně širší vedení organizace rozhoduje na základě konsolidovaných informací.

Tato metodika podporuje:

- sdílené porozumění rizikům,
- vyšší kvalitu rozhodování,
- a udržitelné řízení rizik správy dat.

7 Navazující dokumenty:

- „Návod pro prioritizaci rizik správy dat“
- „Příloha – hodnotící otázky dopadů“
- „Katalog hrozeb a rizik správy dat“
- „Návod pro práci s Excel katalogem“
- „Krátký návod pro práci s Excel katalogem“
- „Příklady využití Katalogu hrozeb a rizik správy dat“