OCHRANA
KRITICKÉ INFRASTRUKTURY

ČR • EU • řízení rizik • odolnost

E-pomůcka pro interní školení

BEZPEČNOST VEŘEJNÁ SPRÁVA OBRANA ŘÍZENÍ RIZIK ODOLNOST

00 Jak s pomůckou pracovat

Materiál propojuje právní požadavky s praktickým řízením rizik a odolnosti.

Pomůcka je určena pro vedoucí pracovníky, manažery rizik a kontinuity, bezpečnostní specialisty, provozovatele technologií, právníky a další osoby, které se podílejí na zachování základních služeb. Lze ji použít jako podklad pro samostudium, dvou – až čtyřhodinové školení nebo jako osnovu interního workshopu.

HLAVNÍ MYŠLENKA
Moderní ochrana kritické infrastruktury se neposuzuje pouze podle toho, zda je chráněn objekt nebo technologie. Rozhodující je schopnost organizace udržet základní službu na přijatelné úrovni, obnovit ji ve stanoveném čase a přizpůsobit se změněným podmínkám.

Výstupy učení

- rozlišit kritickou infrastrukturu, kritický subjekt, základní službu a kritického dodavatele;
- orientovat se ve vazbách mezi českým zákonem o kritické infrastruktuře, CER, NIS2 a českým zákonem o kybernetické bezpečnosti;
- vysvětlit proces posouzení rizik, business impact analysis a tvorby plánu odolnosti;
- identifikovat mezisektorové, dodavatelské, personální, fyzické, informační a technologické závislosti;
- navrhnout praktický plán implementace, testování a průběžného zlepšování odolnosti.

Doporučené použití při školení

Čas	Blok	Doporučený obsah
20 min	**Úvod**	Pojmy, vývoj od ochrany prvku k odolnosti služby.
35 min	**Právní rámec**	Česká úprava, CER, NIS2 a sektorová pravidla.
45 min	**Rizika a odolnost**	Scénáře, závislosti, kaskádové dopady, BIA, kontinuita.
40 min	**Workshop**	Případová studie, kontrolní otázky a návrh 90denního plánu.

01 Obsah

Kliknutím na název přejdete v dokumentu na příslušnou kapitolu.

AKTUALIZAČNÍ POZNÁMKA

Právní a metodický rámec se rychle vyvíjí. Před použitím pro právní posouzení nebo audit vždy ověřte aktuální znění předpisů v e-Sbírce, EUR-Lexu a na portálech HZS ČR a NÚKIB.

02 Co se v systému změnilo

Posun od ochrany jednotlivého prvku ke schopnosti poskytovat základní službu.

Nový český zákon č. 266/2025 Sb. transponuje evropskou směrnici CER. Systém se více orientuje na služby, jejich význam pro společnost a stát, na rizika ze všech relevantních zdrojů a na schopnost subjektu narušení zvládnout. Zásadní není pouze vlastnictví technického prvku, ale především postavení poskytovatele základní služby a význam případného narušení.

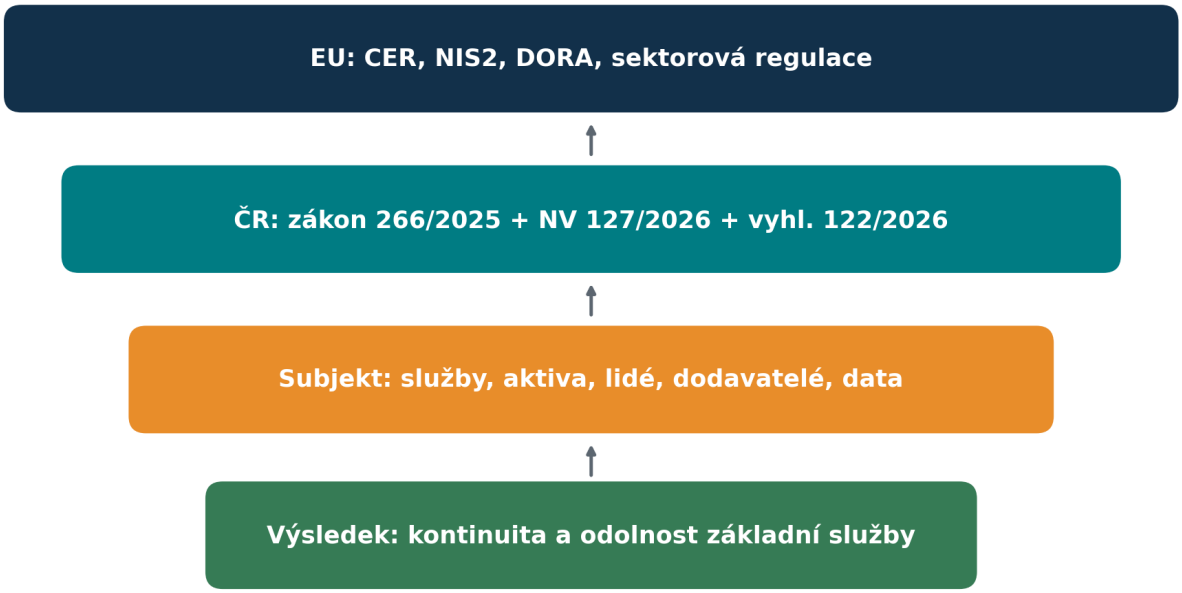


Schéma 1 – vrstvy regulace a praktické implementace

Pět praktických posunů

#	Posun	Dopad pro organizaci
1	**Služba před aktivem**	Předmětem ochrany je kontinuita základní služby. Aktiva jsou prostředkem, nikoli konečným cílem.
2	**All-hazards přístup**	Posuzují se přírodní, technologické, úmyslné, personální, kybernetické i dodavatelské scénáře.
3	**Závislosti a kaskády**	Nutné je sledovat vnitřní, mezisektorové, přeshraniční a dodavatelské vazby.
4	**Měřitelná kontinuita**	Organizace stanoví minimální úroveň služby, priority obnovy a časové cíle.
5	**Odpovědnost vedení**	Odolnost musí být řízena, financována, testována a pravidelně vyhodnocována.

Doporučená literatura a zdroje

- Zákon č. 266/2025 Sb. – zákon o kritické infrastruktuře — základní český předpis
- Směrnice (EU) 2022/2557 – CER — evropský rámec odolnosti kritických subjektů

03 Základní pojmy a systémový pohled

Společný jazyk je podmínkou správného řízení rizik.

Základní služba	Služba zásadní pro zachování životně důležitých společenských funkcí, hospodářských činností, veřejného zdraví, bezpečnosti nebo životního prostředí.
Subjekt kritické infrastruktury	Poskytovatel základní služby, který je určen příslušným postupem a splňuje zákonné podmínky významnosti.
Kritická infrastruktura subjektu	Aktiva, zařízení, systémy, sítě, objekty a další zdroje nezbytné pro poskytování základní služby.
Kritický dodavatel	Dodavatel, jehož služba, produkt, technologie nebo kapacita je zásadní pro udržení nebo obnovu základní služby.
Incident	Událost, která narušuje nebo může narušit poskytování základní služby.
Odolnost	Schopnost předvídat, předcházet, chránit se, reagovat, absorbovat dopady, obnovit činnost a přizpůsobit se.

Systémový pohled: co je nutné mapovat

- služby a procesy – co musí organizace dodávat a komu;
- lidé a znalosti – klíčové role, zastupitelnost, externí specialisté a oprávnění;
- objekty a technologie – provozy, zařízení, OT/ICS, ICT, komunikační systémy a data;
- vstupy – energie, voda, materiál, logistika, finance, licence a veřejné služby;
- dodavatelé a partneři – smlouvy, subdodavatelé, koncentrace trhu, geopolitické a právní závislosti;
- výstupy a odběratelé – dopad narušení na obyvatelstvo, veřejnou správu, jiné sektory a přeshraniční služby.

KONTROLNÍ OTÁZKA

Dokáže organizace určit, která konkrétní kombinace lidí, technologií, dat, energií a dodavatelů je nezbytná pro každou prioritní službu? Pokud ne, nelze spolehlivě posoudit riziko ani navrhnout obnovu.

04 Právní rámec České republiky

Tři základní předpisy tvoří jeden provázaný implementační celek.

1 **Zákon č. 266/2025 Sb.**
stanoví systém, určování subjektů, povinnosti, odpovědnosti, kontrolu a sankce

2 **Nařízení vlády č. 127/2026 Sb.**
vymezuje základní služby a kritéria významnosti pro určení subjektů

3 **Vyhláška č. 122/2026 Sb.**
rozpracovává posouzení rizik, plán odolnosti, opatření a hlášení incidentů

Typické povinnosti subjektu

- zpracovat a pravidelně aktualizovat posouzení rizik;
- zpracovat plán odolnosti navazující na zjištěná rizika;
- určit manažera kritické infrastruktury a odpovědnosti uvnitř organizace;
- určit vlastní kritickou infrastrukturu a kritické dodavatele;
- zavést přiměřená technická, bezpečnostní a organizační opatření;
- zajistit kontinuitu činností a schopnost obnovy základní služby;
- hlásit relevantní incidenty a spolupracovat s orgány veřejné moci;
- ověřovat spolehlivost vybraných osob, provádět školení a účastnit se cvičení.

PRAKTICKÉ PRAVIDLO
Zákon říká „co“ má organizace plnit, nařízení vlády pomáhá určit „koho“ se systém týká a vyhláška rozpracovává „jak“ dokumentovat rizika, plánovat opatření a hlásit incidenty.

Doporučená literatura a zdroje

HZS ČR – Kritická infrastruktura — rozcestník, metodika k zařazení a aktuální informace

HZS ČR – Představení zákona o kritické infrastruktuře — výklad hlavních povinností

HZS ČR – stanovisko a metodika k poskytování informací — aplikační informace pro poskytovatele základních služeb

05 Právní rámec Evropské unie

CER vytváří obecný rámec; NIS2, DORA a sektorové předpisy jej doplňují.

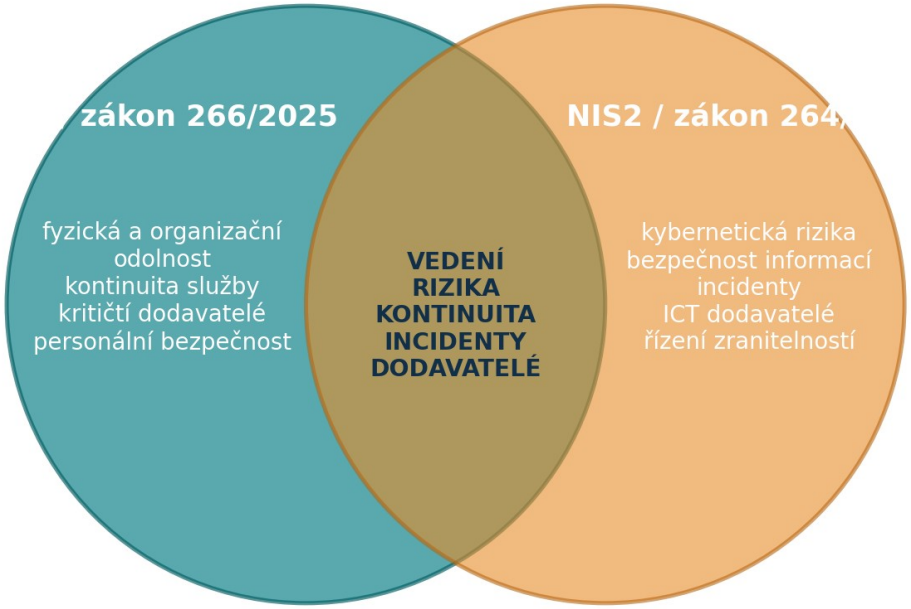


Schéma 2 – společné a specifické oblasti CER a NIS2

Klíčové dokumenty EU

Dokument	Hlavní využití	Odkaz
Směrnice CER – (EU) 2022/2557	základní rámec odolnosti kritických subjektů	**otevřít**
Nařízení v přenesené pravomoci (EU) 2023/2450	nevyčerpávající seznam základních služeb	**otevřít**
Pokyny Komise C/2025/4990	identifikace kritických subjektů a významnosti	**otevřít**
Pokyny Komise C/2026/3712	opatření k zajištění odolnosti podle článku 13 CER	**otevřít**
Směrnice NIS2 – (EU) 2022/2555	řízení kybernetických rizik a incidentů	**otevřít**
Nařízení DORA – (EU) 2022/2554	digitální provozní odolnost finančního sektoru	**otevřít**

POZOR NA SOUBĚH REGULACÍ
Jedna organizace může současně plnit povinnosti podle CER/českého zákona o kritické infrastruktuře, NIS2/českého zákona o kybernetické bezpečnosti, DORA nebo sektorových předpisů. Dokumentace a procesy by proto měly být integrovány, aby se rizika, incidenty a kontinuita neřídily odděleně.

06 Řízení rizik kritické infrastruktury

Posouzení musí vycházet z kontextu služby, scénářů, závislostí a reálných dopadů.

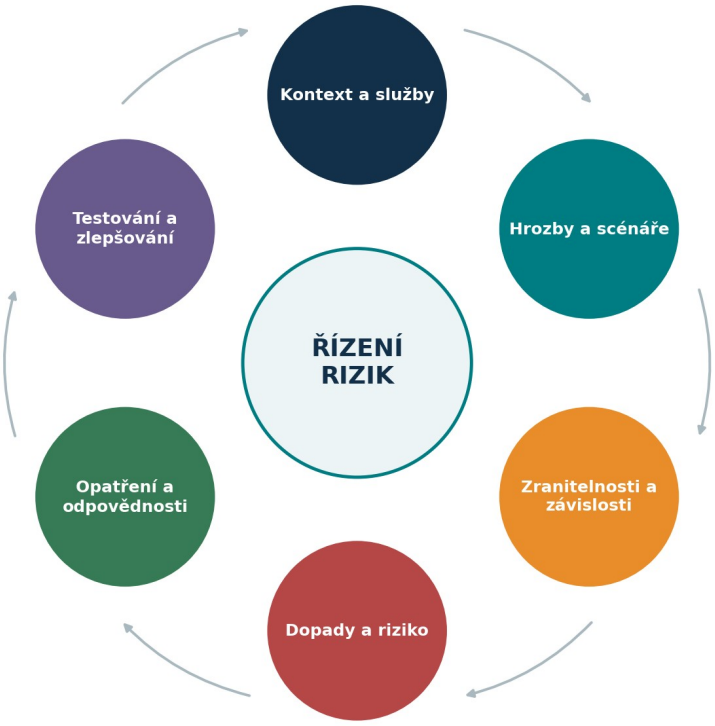


Schéma 3 – opakující se cyklus řízení rizik

Doporučený postup posouzení

1. **Vymezit rozsah:** základní služba, procesy, geografický a organizační rozsah, časový horizont a zainteresované strany.
2. **Stanovit kritéria:** stupnice pravděpodobnosti a dopadu, tolerance rizika, prahové hodnoty a pravidla eskalace.
3. **Tvořit scénáře:** přírodní, technologické, úmyslné, personální, kybernetické, dodavatelské a kombinované události.
4. **Mapovat závislosti:** energie, voda, ICT/OT, data, komunikace, logistika, pracovníci, finance, dodavatelé a veřejné služby.
5. **Hodnotit dopady:** bezpečnost osob, dostupnost služby, ekonomika, veřejná důvěra, životní prostředí a přeshraniční účinky.
6. **Určit opatření:** prevence, ochrana, redundance, substituce, zásoby, reakce, kontinuita, obnova a adaptace.
7. **Určit vlastníka:** odpovědnost za riziko, financování, termín, indikátory a způsob ověření účinnosti.
8. **Testovat a aktualizovat:** cvičení, incidenty, změny hrozeb, dodavatelů, technologie, procesů a právních požadavků.

Kaskádové a systémové dopady

Narušení jedné služby může způsobit selhání dalších služeb. Proto nestačí hodnotit každé aktivum izolovaně. Analýza musí zachytit směr závislosti, její sílu, časovou citlivost, existenci náhrady a bod, kdy lokální porucha přechází v sektorový nebo společenský problém.

Závislost	Kontrolní otázka	Možné opatření	Indikátor
Elektrická energie	Jak dlouho lze službu udržet bez sítě?	záložní napájení, palivo, priorita obnovy	hodiny autonomie
ICT/komunikace	Existuje nezávislý komunikační kanál?	redundantní spojení, offline postupy	RTO, dostupnost
Dodavatel	Je dostupná náhrada nebo zásoba?	dual sourcing, escrow, zásoby	doba substituce
Lidé	Které role nemají zastupitelnost?	cross-training, pohotovost, smluvní záloha	počet zastupitelných rolí

Doporučená literatura a zdroje

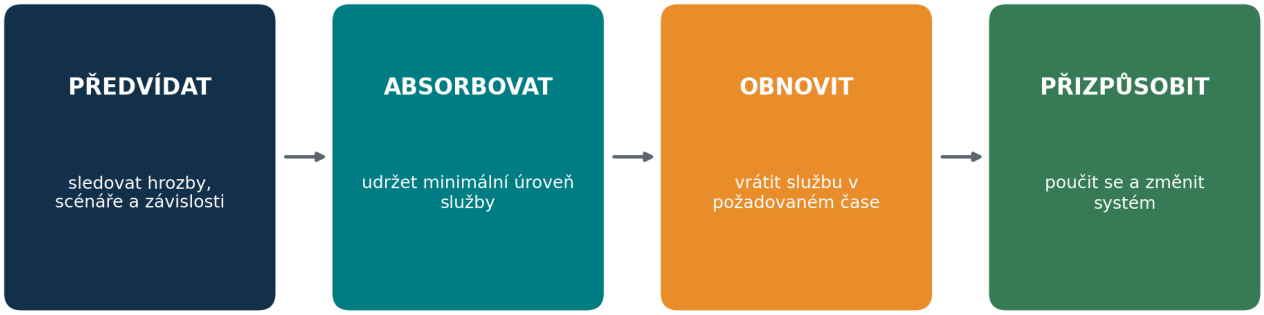
ISO 31000:2018 – Risk management — Guidelines — principy, rámec a proces řízení rizik

IEC 31010:2019 – Risk assessment techniques — výběr analytických technik

JRC – CRISRRAM — metodika posouzení rizik kritické infrastruktury

07 Odolnost a kontinuita základní služby

Odolnost propojuje prevenci, absorpci dopadu, obnovu a adaptaci.



Odolnost je schopnost zachovat nebo rychle obnovit základní službu - nikoli pouze ochránit jednotlivé aktivum.

Schéma 4 – čtyři schopnosti odolného systému

Od rizika ke konkrétním časovým cílům

MTPD / MTPoD	maximální tolerovatelná doba narušení – bod, po kterém jsou dopady pro organizaci nebo společnost nepřijatelné
RTO	cílová doba obnovy procesu, služby nebo technologie
RPO	maximální přijatelná ztráta dat vyjádřená časem
Minimální úroveň služby	nejnižší výkon nebo kapacita, kterou je nutné během narušení zachovat
Priorita obnovy	pořadí procesů, aktiv a zdrojů podle dopadu a časové kritičnosti

Co musí obsahovat strategie kontinuity

- jasné priority základních služeb a minimální provozní režimy;
- varianty práce při výpadku hlavních objektů, technologií, komunikace nebo personálu;
- redundanci, diverzifikaci a substituci kritických zdrojů;
- postupy aktivace, rozhodovací pravomoci a komunikační pravidla;
- obnovu dat, technologií, provozů a dodavatelských kapacit;
- návrat do standardního režimu a následné vyhodnocení incidentu.

NEZAMĚŇOVAT
Disaster recovery se obvykle zaměřuje na obnovu ICT. Business continuity řeší udržení prioritních procesů. Odolnost je ještě širší: zahrnuje prevenci, ochranu, reakci, obnovu, adaptaci a schopnost fungovat v nejistotě.

Doporučená literatura a zdroje

ISO 22301:2019 – Business continuity management systems — požadavky na systém managementu kontinuity

ISO/TS 22317:2021 – Business impact analysis — metodika BIA a časové priority

ISO 22316:2017 – Organizational resilience — principy organizační odolnosti

ISO 22372:2025 – Guidelines for infrastructure resilience — novější rámec odolnosti infrastruktury

08 CER, NIS2 a kybernetická/OT bezpečnost

Fyzická a kybernetická odolnost jsou dvě části jednoho provozního systému.

V kritické infrastruktuře jsou digitální systémy pevně propojeny s fyzickými procesy. Výpadek identity managementu, telekomunikačního spojení, cloudové služby, řídicího systému nebo dodavatelské podpory může mít okamžitý dopad na fyzický provoz a bezpečnost osob. Proto je nutné spojit řízení rizik CER s požadavky NIS2 a s bezpečností průmyslových řídicích systémů.

Integrované oblasti řízení

GOVERNANCE
společný výbor nebo jasně propojené role pro bezpečnost, rizika, kontinuitu, ICT a provoz

AKTIVA A SLUŽBY
jedna vazba mezi základní službou, procesem, IT/OT aktivem, objektem a dodavatelem

RIZIKA
společný registr scénářů a závislostí; odlišení dopadů na důvěrnost, integritu, dostupnost a bezpečnost provozu

INCIDENTY
společné situační povědomí, eskalace, rozhodování a koordinované splnění ohlašovacích povinností

DODAVATELÉ
hodnocení ICT, OT i fyzických dodavatelů, subdodavatelů, vzdáleného přístupu a ukončení smlouvy

TESTOVÁNÍ
technické testy, tabletop cvičení, obnovy záloh, výpadky komunikace a kombinované scénáře

Doporučená literatura a zdroje

Zákon č. 264/2025 Sb., o kybernetické bezpečnosti — česká transpozice NIS2

Portál NÚKIB – podpůrné materiály — metodiky, manuály a výklady

ENISA – NIS2 Technical Implementation Guidance — praktická technická implementace

IEC 62443 – Security for industrial automation and control systems — rodina norem pro OT/ICS

ISO/IEC 27005:2022 – Information security risk management — řízení informačních bezpečnostních rizik

09 Plán odolnosti a governance

Plán musí být řídicím nástrojem, nikoli pouze formální dokumentací.

Doporučená struktura plánu odolnosti

Část	Minimální obsah
1. Kontext a rozsah	základní služby, organizační rozsah, právní působnost, zainteresované strany
2. Governance	odpovědnost vedení, manažer kritické infrastruktury, krizové role a zastupitelnost
3. Výsledky posouzení rizik	scénáře, zranitelnosti, závislosti, kritérium přijatelnosti a priority
4. Kritická infrastruktura a dodavatelé	mapa aktiv, procesů, lokalit, technologií a externích kapacit
5. Opatření	fyzická, personální, organizační, provozní, kybernetická a dodavatelská opatření
6. Kontinuita a obnova	minimální úrovně služby, RTO/RPO, zdroje, alternativy a návrat do standardu
7. Incident management	detekce, klasifikace, eskalace, komunikace, hlášení a spolupráce
8. Výcvik a cvičení	kompetence, školení, scénáře, frekvence, dokumentace a lessons learned
9. Metriky a aktualizace	KPI/KRI, audit, změnové spouštěče a schvalování aktualizací

Role vedení

- schválit rozsah systému, kritéria rizika a toleranci narušení;
- určit vlastníky základních služeb a rizik, nikoli ponechat odpovědnost pouze bezpečnostnímu útvaru;
- alokovat zdroje podle skutečné kritičnosti a ověřeného snížení rizika;
- vyžadovat pravidelné informace o vývoji rizik, nedostatcích, incidentech a výsledcích cvičení;
- řešit konflikty mezi efektivitou, náklady, rychlostí a požadovanou redundancí.

MĚŘÍTKO KVALITY
Kvalitní plán odolnosti umožní odpovědné osobě během incidentu rychle zjistit: co je prioritou, kdo rozhoduje, jaké zdroje jsou dostupné, co se má aktivovat, koho informovat a podle čeho poznat, že obnova postupuje správně.

Doporučená literatura a zdroje

- Vyhláška č. 122/2026 Sb. — obsah posouzení, plánu, opatření a hlášení
- Pokyny Komise C/2026/3712 — doporučení k technickým, bezpečnostním a organizačním opatřením

10 Incidenty, cvičení a průběžné zlepšování

Odolnost nelze prokázat pouze existencí dokumentu; musí být testována.

Životní cyklus incidentu

Detekce **monitoring, hlášení zaměstnanců, dodavatelů a veřejných orgánů**	**Klasifikace** **dopad na základní službu, trend, geografický a přeshraniční rozsah**	**Aktivace** **krizový tým, kontinuita, náhradní provoz, ochranná opatření**
Komunikace interní tok informací, regulátor, veřejnost, zákazníci a partneři	**Obnova** priority, ověření bezpečnosti, návrat kapacity, dočasná a trvalá řešení	**Vyhodnocení** kořenová příčina, účinnost opatření, lessons learned a aktualizace rizik

Portfolio testů a cvičení

Typ	Co ověřuje	Orientace
Kontrola dokumentace	ověřit kontakty, role, smlouvy, alternativní postupy a dostupnost zdrojů	čtvrtletně
Tabletop cvičení	vedení a klíčové role řeší scénář bez reálného přerušení	1-2× ročně
Technický test	zálohy, alternativní napájení, komunikace, failover, OT/ICT obnova	podle kritičnosti
Provozní cvičení	reálný přechod na náhradní proces nebo lokalitu	alespoň ročně u prioritních služeb
Mezisektorové cvičení	společný scénář s dodavateli, veřejnou správou a dalšími sektory	podle rizika
Stress test	extrémní, kombinovaný nebo dlouhodobý scénář překračující běžné předpoklady	periodicky / po změně hrozeb

LESSONS LEARNED
Každé cvičení a významný incident musí skončit seznamem zjištění, vlastníkem nápravného opatření, termínem, zdroji a ověřením, že opatření skutečně snížilo riziko. Bez uzavření tohoto cyklu se organizace nepoučí.

Doporučená literatura a zdroje

- EU Critical Infrastructure Blueprint — koordinace při závažných přeshraničních incidentech
- ISO 22361:2022 – Crisis management — strategické krizové řízení a rozhodování
- JRC – Towards Testing Critical Infrastructure Resilience — testování a stress testy

11 Implementační cestovní mapa

Praktický rámec pro první rok budování systému.

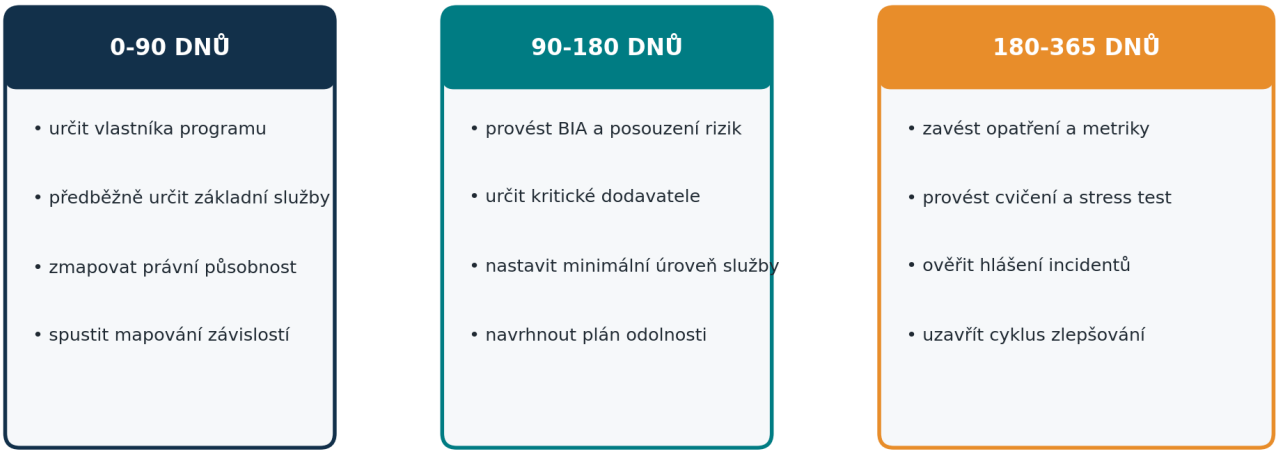


Schéma 5 – doporučené pořadí implementačních kroků

Rozhodovací milníky

- Milník 1 – rozsah potvrzen: Je jasné, které služby a organizační části spadají do systému a kdo je jejich vlastníkem.
- Milník 2 – rizika prioritizována: Existuje schválené posouzení hlavních scénářů, závislostí a nepřijatelných dopadů.
- Milník 3 – obnova definována: Jsou stanoveny minimální úrovně služby, RTO/RPO, zdroje a alternativní režimy.
- Milník 4 – opatření financována: Vedení schválilo portfolio opatření, vlastníky, harmonogram a metriky.
- Milník 5 – systém ověřen: Proběhlo cvičení nebo test, zjištění byla vyřešena a dokumentace aktualizována.

DOPORUČENÍ PRO ŘÍZENÍ PROJEKTU
Nevytvářejte oddělené projekty „CER“, „NIS2“, „BCM“ a „fyzická bezpečnost“, pokud se týkají stejných služeb. Vytvořte společnou architekturu služeb, aktiv, rizik, incidentů a odpovědností; specifické povinnosti řešte jako pohledy nad stejným systémem.

12 Workshop a kontrolní seznam

Přenos principů do konkrétní organizace.

Případová studie: výpadek základní služby

SCÉNÁŘ

V důsledku extrémního počasí dochází k dlouhodobému výpadku elektřiny a telekomunikací. Současně je omezen příjezd zaměstnanců, hlavní dodavatel hlásí nedostupnost technické podpory a v řídicím systému se objevují nestandardní události. Organizace musí udržet alespoň 40 % kapacity základní služby po dobu 72 hodin.

Úkol pro skupiny

1. Určete pět nejkritičtějších závislostí a vysvětlete, jak se mohou projevit v čase.
2. Stanovte rozhodovací body pro 0-2 hodiny, 2-12 hodin, 12-24 hodin a 24-72 hodin.
3. Navrhněte minimální úroveň služby a pořadí obnovy procesů.
4. Určete, které informace potřebuje vedení, regulátor, zaměstnanci, dodavatelé a veřejnost.
5. Navrhněte tři okamžitá, tři střednědobá a tři systémová opatření.

Rychlý kontrolní seznam organizace

✓	Oblast	Kontrolní otázka
☐	**Právní působnost**	Máme ověřeno, které základní služby poskytujeme a jaká kritéria významnosti mohou být relevantní?
☐	**Vlastnictví**	Má každá prioritní služba vlastníka s pravomocí rozhodovat o riziku a zdrojích?
☐	**Závislosti**	Je služba propojena s procesy, lidmi, objekty, IT/OT, daty, energií a dodavateli?
☐	**Rizika**	Obsahuje posouzení kombinované a kaskádové scénáře, nikoli jen seznam hrozeb?
☐	**Kontinuita**	Jsou stanoveny minimální úrovně služby, RTO/RPO a alternativní postupy?
☐	**Dodavatelé**	Známe subdodavatele, koncentraci, náhrady, exit plán a podmínky vzdáleného přístupu?
☐	**Incidenty**	Je jasné, kdo klasifikuje incident, aktivuje plány a plní ohlašovací povinnosti?
☐	**Cvičení**	Byl systém prakticky ověřen a byla zjištění uzavřena?
☐	**Metriky**	Vedení sleduje indikátory rizika, připravenosti, kapacity obnovy a stav opatření?

12 A Rychlé odkazy pro účastníky

Naskenujte QR kód nebo klikněte na název zdroje.

HZS: kritická infrastruktura	Směrnice CER	Pokyny Komise 2026

13 Katalog odborných zdrojů

Výběr ověřených právních, metodických, normativních a odborných materiálů.

Každá položka obsahuje přímý aktivní odkaz a stručné doporučení k použití. Právní předpisy vždy čtěte v aktuálním znění. U technických norem jsou plná znění zpravidla zpoplatněna; odkazy vedou na oficiální anotace vydavatelů.

A. Česká legislativa a oficiální metodiky

- **Zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury** — základní český právní rámec.
- **Nařízení vlády č. 127/2026 Sb., o základních službách a kritériích významnosti** — určení služeb a významnosti.
- **Vyhláška č. 122/2026 Sb., o plánu odolnosti, posouzení rizik, opatřeních a hlášení** — praktické požadavky na dokumentaci a opatření.
- **HZS ČR – Kritická infrastruktura — hlavní odborný rozcestník.**
- **HZS ČR – Představení zákona o kritické infrastruktuře** — stručný oficiální výklad.
- **HZS ČR – metodika k zařazení poskytovatele základní služby** — postup poskytovatele a informační povinnost.
- **HZS ČR – Klíčové nařízení vlády o subjektech kritické infrastruktury** — vysvětlení NV 127/2026.
- **Bezpečnostní strategie České republiky 2023** — národní bezpečnostní kontext.
- **Přehled významných bezpečnostních dokumentů ČR** — oficiální rozcestník strategických dokumentů.
- **Analýza hrozeb pro Českou republiku** — výchozí národní katalog rizik a scénářů.
- **HZS ČR – vzdělávací moduly krizového řízení, včetně Modulu I** — studijní materiály ke kritické infrastruktuře.

B. Kybernetická bezpečnost v ČR

- **Zákon č. 264/2025 Sb., o kybernetické bezpečnosti** — český rámec NIS2.
- **NÚKIB – Průvodce novým zákonem o kybernetické bezpečnosti** — aplikační průvodce.
- **NÚKIB – podpůrné materiály — praktické manuály a metodiky.**
- **NÚKIB – hlášení kybernetických bezpečnostních incidentů** — postup hlášení incidentů.
- **NÚKIB – řízení bezpečnostní politiky a dokumentace** — vzorová struktura dokumentace.
- **NÚKIB – přiměřenost bezpečnostních opatření** — rizikově orientované zavádění opatření.

C. Evropská unie

- **Směrnice (EU) 2022/2557 – CER — odolnost kritických subjektů.**
- **Nařízení Komise v přenesené pravomoci (EU) 2023/2450** — seznam základních služeb.
- **Pokyny Komise C/2025/4990 — identifikace kritických subjektů.**
- **Pokyny Komise C/2026/3712 — opatření k zajištění odolnosti.**
- **Evropská komise – Critical infrastructure resilience at EU level** — hlavní evropský rozcestník.
- **Doporučení Rady 2023/C 20/01** — koordinovaný přístup a zátěžové testy.
- **EU Critical Infrastructure Blueprint** — koordinace závažných přeshraničních incidentů.
- **Směrnice (EU) 2022/2555 – NIS2 — kybernetická rizika a incidenty.**
- **Prováděcí nařízení Komise (EU) 2024/2690** — technické požadavky pro vybrané digitální subjekty.
- **ENISA – NIS2 Technical Implementation Guidance** — praktická implementace NIS2.
- **Nařízení (EU) 2022/2554 – DORA** — digitální provozní odolnost finančního sektoru.

D. Metodiky a odborné studie

- **JRC – Critical Entities Resilience — výzkumný rozcestník.**
- **JRC – CRISRRAM — posouzení rizik kritické infrastruktury.**
- **JRC – Risk Assessment Methodology for Critical Infrastructure Protection** — strukturovaná analýza rizik.
- **JRC – Risk Assessment and Resilience for Critical Infrastructures** — propojení rizik a resilience.

- **JRC – From Risk Management to Resilience** — posun k systémové odolnosti.
- **JRC – Towards Testing Critical Infrastructure Resilience** — cvičení a stress testy.
- **JRC – Natech risks** — technologické havárie vyvolané přírodními jevy.
- **VŠB-TUO – Metodický postup posilování resilience kritických subjektů** — česká aplikovaná metodika.
- **VŠB-TUO – databáze procesů obnovy — podpora analýzy obnovy.**
- **OECD – Good Governance for Critical Infrastructure Resilience** — governance a partnerství státu s provozovateli.
- **OECD – Ensuring the resilience of critical infrastructure 2025** — aktuální mezinárodní srovnání governance.
- **OECD Recommendation on the Governance of Critical Risks** — národní řízení kritických rizik.
- **UNDRR – Principles for Resilient Infrastructure** — globální principy odolné infrastruktury.
- **UNDRR – Handbook for Implementing the Principles** — praktická implementační příručka.
- **Sendai Framework 2015–2030** — globální rámec snižování rizika katastrof.
- **European Climate Risk Assessment – EUCRA** — klimatická rizika pro evropskou infrastrukturu.

E. Technické normy

- **ISO 31000:2018 – Risk management — Guidelines — řízení rizik.**
- **ISO – bezplatný přehled ISO 31000 — stručný úvod.**
- **IEC 31010:2019 – Risk assessment techniques — analytické techniky.**
- **ISO 22301:2019 – Business continuity management systems** — management kontinuity.
- **ISO 22313:2020 – Guidance on the use of ISO 22301** — implementace BCM.
- **ISO/TS 22317:2021 – Business impact analysis — BIA.**
- **ISO 22316:2017 – Organizational resilience — organizační odolnost.**
- **ISO 22361:2022 – Crisis management — krizové řízení.**
- **ISO 22342:2023 – Guidelines for security plans** — bezpečnostní plány.
- **ISO 22372:2025 – Guidelines for infrastructure resilience** — odolnost infrastruktury.
- **ISO/IEC 27001:2022 – Information security management systems** — ISMS.
- **ISO/IEC 27005:2022 – Information security risk management** — informační rizika.
- **IEC 62443 – Industrial automation and control systems security** — OT/ICS bezpečnost.

F. Sektorové a širší strategické zdroje

- **Nařízení (EU) 2019/941 – riziková připravenost v elektroenergetice** — elektřina.
- **Nařízení (EU) 2017/1938 – bezpečnost dodávek zemního plynu — plyn.**
- **Směrnice 2007/60/ES – povodňová rizika — povodně.**
- **Směrnice 2012/18/EU – Seveso III — závažné průmyslové havárie.**
- **Nařízení (EU) 2022/2371 – přeshraniční zdravotní hrozby** — zdravotnictví.
- **Evropská strategie odolnosti vodních zdrojů — vodní odolnost.**
- **Akční plán EU pro bezpečnost podmořských kabelů** — podmořská digitální infrastruktura.
- **EU Preparedness Union Strategy — celospolečenská připravenost EU.**
- **Safer Together – Niinistö Report — civilní a vojenská připravenost.**

14 Slovník klíčových pojmů

Pracovní definice pro školení a interní komunikaci.

Pojem	Význam
All-hazards approach	posuzování všech relevantních typů hrozeb a jejich kombinací, nikoli pouze jednoho druhu ohrožení
BIA	business impact analysis; určení dopadů přerušení, priorit a časových požadavků na obnovu
CER	směrnice EU o odolnosti kritických subjektů
Kaskádový dopad	šíření poruchy mezi aktivy, procesy, sektory nebo územími
KRI	key risk indicator; ukazatel změny nebo růstu rizika
MTPD	maximální tolerovatelná doba narušení
NIS2	směrnice EU o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti
OT / ICS / SCADA	provozní technologie a řídicí systémy fyzických procesů
RPO	cílový bod obnovy dat, tedy přijatelný rozsah ztráty dat vyjádřený časem
RTO	cílová doba obnovy služby, procesu nebo systému
Resilience	schopnost předvídat, odolávat, absorbovat, reagovat, obnovit se a adaptovat
Stress test	zkouška chování systému v extrémních nebo kombinovaných podmínkách
Základní služba	služba zásadní pro zachování významných společenských a ekonomických funkcí

ZÁVĚR

Odolnost kritické infrastruktury není jednorázový projekt ani soubor samostatných bezpečnostních opatření. Je to průběžně řízená schopnost organizace poskytovat prioritní služby navzdory narušení a proměňujícím se podmínkám.