Spolufinancováno Evropskou unií

KyBez Handbook

Obsah

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Úvod

Účel dokumentu

Tento handbook vzniká v rámci projektu CYLANCES jako praktický průvodce pro organizace při zavádění a rozvoji kybernetické bezpečnosti v souladu s požadavky směrnice NIS2 a související národní legislativy.

Cílem dokumentu není nahrazovat právní předpisy ani detailní technické standardy, ale poskytnout srozumitelný a prakticky využitelný rámec, který organizacím pomůže:

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- pochopit základní požadavky v oblasti kybernetické bezpečnosti,
- identifikovat klíčová rizika a slabá místa,
- zavádět odpovídající bezpečnostní opatření,
- a nastavit procesy, které povedou k dlouhodobému zvyšování odolnosti organizace.

Dokument je koncipován tak, aby byl použitelný napříč různými typy organizací, zejména s ohledem na jejich velikost, sektor a úroveň vyspělosti v oblasti kybernetické bezpečnosti.

Rozsah a cílová skupina

Handbook je určen především institucím a osobám zapojeným do projektu CYLANCES, a to subjektům veřejného sektoru, organizacím spadajícím do regulace podle NIS2, malým a středním podnikům zavádějícím základní bezpečnostní opatření, a osobám odpovědným za kybernetickou bezpečnost (manažeři kybernetické bezpečnosti, IT vedoucí, odpovědné osoby).

Obsah dokumentu se zaměřuje na praktické aspekty řízení kybernetické bezpečnosti, zejména:

- řízení rizik,
- zavádění bezpečnostních opatření,
- řízení dodavatelských vztahů,
- a zvládání bezpečnostních incidentů.

Technicky detailní implementace jednotlivých opatření není předmětem tohoto dokumentu a je ponechána na konkrétních potřebách organizace.

Vztah k legislativě a regulatorním požadavkům

Tento handbook vychází z požadavků směrnice NIS2 a souvisejících národních právních předpisů, zejména v oblastech:

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- řízení rizik,
- zavádění bezpečnostních opatření,
- řízení dodavatelských vztahů,
- a hlášení a řešení kybernetických incidentů.

Jednotlivé kapitoly dokumentu reflektují tyto požadavky a převádějí je do praktické podoby, kterou lze aplikovat v běžném provozu organizace.

Dokument neobsahuje úplný výčet legislativních povinností ani jejich právní výklad. Organizace by proto měly vždy zohlednit aktuální znění relevantních právních předpisů a případně využít odborné konzultace.

Jak dokument používat

Handbook je navržen jako praktický pracovní nástroj, nikoli jako lineární text určený k jednorázovému přečtení. Tento handbook je koncipován jako živý dokument, který bude průběžně aktualizován a rozšiřován po celou dobu trvání projektu CYLANCES.

Doporučený postup práce s dokumentem:

- využít “Checklist minimálních opatření” pro orientační posouzení aktuálního stavu,
- identifikovat relevantní oblasti podle charakteru organizace,
- postupně zavádět opatření podle priorit,
- a využívat přiložené nástroje (checklisty, matice, vzory) při implementaci.

Dokument zároveň respektuje princip přiměřenosti – ne všechna opatření jsou vhodná pro všechny organizace ve stejném rozsahu. Každá organizace by měla přizpůsobit implementaci svým konkrétním podmínkám, rizikům a kapacitám.

Cílem je, aby handbook reflektoval aktuální potřeby praxe a poskytoval stále relevantní a použitelné informace, nikoli statický soubor doporučení.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Rozdělení na režim vyšších a nižších povinností

Zákon č. 264/2025 Sb. o kybernetické bezpečnosti rozlišuje dvě základní úrovně regulace:

- režim nižších povinností, upravený Vyhláškou č. 410/2025 Sb.
- režim vyšších povinností, upravený Vyhláškou č. 409/2025 Sb.

Rozdělení vychází z významu poskytované služby a dopadu jejího narušení.
Režim nižších povinností představuje minimální úroveň zabezpečení, zatímco režim vyšších povinností zavádí systematické řízení kybernetické bezpečnosti.

Oba režimy jsou založeny na principu řízení rizik a přiměřenosti bezpečnostních opatření.

Liší se však:

- rozsahem povinností,
- mírou formalizace,
- požadavky na dokumentaci a řízení.

Přehled hlavních rozdílů:

Oblast	**Nižší režim**	**Vyšší režim**
Přístup	Minimální bezpečnostní opatření	Systém řízení bezpečnosti informací
Formalizace	Nízká	Vysoká
Dokumentace	Základní	Povinná a systematická
Řízení rizik	Nepřímo se zohledněním potřeb	Povinné, metodické
Audit	Není explicitně vyžadován	Povinný
Role	Minimální požadavky	Definované bezpečnostní

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

		role
Dodavatelé	Základní smluvní požadavky	Řízení dodavatelských rizik

Režim nižších povinností

Režim nižších povinností je upraven vyhláškou č. 410/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

Jeho cílem je zajistit minimální úroveň kybernetické bezpečnosti odpovídající významu regulované služby.

Organizace v nižším režimu musí minimálně zajistit:

- přehled aktiv,
- základní bezpečnostní dokumentaci,
- evidenci bezpečnostních opatření včetně odůvodnění jejich zavedení či nezavedení,
- proces řešení kybernetických bezpečnostních incidentů,
- základní řízení vztahů s dodavateli.

Příkladem může být seznam systémů a služeb, jednoduchý plán obnovy, školení zaměstnanců či evidence bezpečnostních opatření (viz tabulka ve vyhlášce).
Povinný základ tvoří zejména:

- systém zajišťování kybernetické bezpečnosti,
- zapojení vrcholného vedení,
- bezpečnost lidských zdrojů,
- řízení kontinuity činností,
- zvládání kybernetických bezpečnostních incidentů.

Další bezpečnostní opatření organizace zavádí na základě přiměřenosti, případně zdůvodní jejich nezavedení. Typicky se jedná o:

- řízení přístupů,
- správu identit,
- detekci událostí,
- bezpečnost sítí,
- aplikační bezpečnost,

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- kryptografii.

Organizace musí být schopna svá rozhodnutí v této oblasti doložit.

Režim vyšších povinností

Režim vyšších povinností je upraven vyhláškou č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Na rozdíl od nižšího režimu vyžaduje zavedení komplexního systému řízení kybernetické bezpečnosti.

Organizace musí zavést a řídit zejména:

- systém řízení bezpečnosti informací,
- řízení rizik,
- řízení aktiv,
- řízení dodavatelů,
- řízení přístupů a identit,
- detekci a vyhodnocování bezpečnostních událostí,
- řízení kybernetických incidentů,
- řízení kontinuity činností,
- audit kybernetické bezpečnosti.

Součástí je povinnost stanovit metodiku řízení rizik, pravidelně provádět hodnocení rizik, zpracovávat plán zvládání rizik a dokumentovat přijatá rozhodnutí.

Audit kybernetické bezpečnosti je prováděn pravidelně, minimálně jednou za dva roky a nezbytné je také přijímání nápravných opatření.

Povinné role a řízení:

Organizace v režimu vyšších povinností stanoví bezpečnostní role, zejména:

- manažera kybernetické bezpečnosti,
- architekta kybernetické bezpečnosti,
- garanta aktiva,

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- auditora kybernetické bezpečnosti.

Současně je povinné zapojení vrcholného vedení a vzniká formální governance (např. výbor KB).

Společné povinnosti obou režimů

Bez ohledu na režim musí organizace:

- zavádí přiměřená bezpečnostní opatření,
- zajišťuje důvěrnost, integritu a dostupnost služeb,
- řeší a hlásí kybernetické bezpečnostní incidenty,
- spolupracuje s příslušnými orgány,
- průběžně vyhodnocuje a zlepšuje stav kybernetické bezpečnosti.

Typické nedostatky v praxi

V praxi se objevuje snaha systém formálně naplnit bez reálného zohlednění bezpečnostních potřeb organizace, díky tomu se často objevují chyby jako:

- **formální existence dokumentace bez reálného provádění procesů** - dokument, který formálně splňuje legislativu sice naplní požadavek, ale bez funkčního procesu v organizaci neposkytuje žádnou ochranu a sám o sobě ani bezpečnost.
- **nepřiměřené zavádění požadavků neodpovídajících velikosti a charakteru organizace** - zde to může vypadat, že více splněných požadavků může znamenat vyšší bezpečnost, opak je ale pravdou, pokud bude např. malá organizace aplikovat nepřiměřené množství požadavků, bude ztrácet přehled a sama sebe brzdit v efektivitě při fungování. Lepší je přiměřené množství požadavků, které organizace procesně zvládá, než velké množství mimo kontrolu a zvládání.
- **nedostatečné zapojení vrcholného vedení** - vedení organizace je nedílnou součástí bezpečnosti. Je přímo odpovědné za její naplňování a kromě toho, spolupráce s vedením může přinést nejen jiný pohled na problematiku, ale také hladší průběh při implementaci.
- **absence evidence zavedených opatření** - nedostatečná evidence opatření nevyhnutelně povede k chaosu. Není možné kontrolovat a naplňovat něco, co nevíme, že je zavedeno.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- **nedostatečné řízení dodavatelských vztahů** - při řízení dodavatelů je důležité spolupracovat a komunikovat. Incident u dodavatele může ohrozit i Vaše data či bezpečnost a bez spolupráce, zasmluvnění a hlavně komunikace se o něm nemusí organizace ani dozvědět, natož reagovat.
- **nefunkční procesy řízení kybernetických incidentů** - u každého incidentu je důležitá reakce a následné kroky. Pokud je řízení incidentů zavedeno pouze formálně a ne procesně, může se stát, že při probíhajícím incidentu nebude správně reagováno a dopady incidentu tak budou vyšší. Může dojít například k výpadku fungování organizace, finančním ztrátám, vydírání či ztrátě dat/know how.

Doporučený postup zavedení

Pro zavedení požadavků je vhodné postupovat následovně:

1. určit příslušný režim povinností,
2. stanovit rozsah řízení kybernetické bezpečnosti,
3. identifikovat aktiva a služby,
4. vytvořit přehled bezpečnostních opatření,
5. zavádět opatření postupně podle priority.

Minimální bezpečnostní základ

Minimální bezpečnostní základ představuje soubor opatření, která by měla být zavedena v každé organizaci bez ohledu na její velikost, sektor nebo zařazení do režimu povinností.

Tato opatření vycházejí z požadavků legislativy a zároveň reflektují běžná rizika, se kterými se organizace v praxi setkávají.

Organizace by měla zajistit alespoň následující oblasti:

a) Přehled aktiv

- identifikace klíčových systémů, služeb a dat,
- určení odpovědnosti za jednotlivá aktiva.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

b) Řízení přístupů

- používání jedinečných přístupových údajů,
- omezení oprávnění na nezbytné minimum,
- zavedení vícefaktorového ověřování tam, kde je to možné.

c) Správa systémů a zařízení

- pravidelná aktualizace systémů a aplikací,
- evidence používaných zařízení,
- omezení používání nepodporovaného software.

d) Ochrana dat

- identifikace citlivých dat,
- omezení přístupu k těmto datům,
- základní pravidla pro jejich sdílení a ukládání.

e) Lidský faktor

- pravidelné školení zaměstnanců,
- stanovení základních pravidel bezpečného chování,
- definovaný postup pro hlášení podezřelých aktivit.

f) Řízení dodavatelů

- přehled dodavatelů s přístupem k systémům nebo datům,
- základní bezpečnostní požadavky ve smlouvách,
- určení odpovědnosti za řízení dodavatelských vztahů.

g) Řízení incidentů

- definovaný postup při bezpečnostním incidentu,
- určení odpovědných osob,
- evidence incidentů.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

h) Kontinuita činností

- základní plán obnovy provozu,
- zálohování klíčových dat,
- ověření obnovitelnosti dat.

Minimální bezpečnostní základ nepředstavuje konečný stav, ale výchozí úroveň. Rozsah a hloubka opatření by měly být dále rozvíjeny na základě řízení rizik a potřeb organizace.

Rychlá sebekontrola (self-assessment)

Rychlá sebekontrola slouží k orientačnímu posouzení aktuální úrovně kybernetické bezpečnosti organizace. Jejím cílem není detailní audit, ale identifikace hlavních nedostatků a stanovení dalšího postupu.

Sebekontrola by měla být provedena formou jednoduchého vyhodnocení základních oblastí:

- **Identifikace aktiv:** Jsou známy klíčové systémy, data a služby?
- **Přístupy a oprávnění:** Jsou přístupy řízené a pravidelně kontrolované?
- **Technická opatření:** Jsou systémy aktualizované a spravované?
- **Lidský faktor:** Jsou zaměstnanci pravidelně školeni?
- **Dodavatelé:** Je známo, kdo má přístup k systémům nebo datům?
- **Incidenty:** Existuje postup pro řešení incidentů?
- **Kontinuita provozu:** Jsou data zálohována a lze je obnovit?

Vyhodnocení a výstup

Každou oblast lze hodnotit například jednoduchým způsobem: splněno, částečně splněno nebo nesplněno. Výsledkem je přehled oblastí, které jsou dostatečně pokryty, vyžadují doplnění, nebo představují kritické riziko.

Výstupem by měl být stručný přehled:

- hlavních nedostatků,
- identifikovaných rizik,

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- doporučených opatření.

Tento přehled slouží jako podklad pro stanovení priorit.

Stanovení priorit

Na základě výsledků sebekontroly je nutné určit pořadí zavádění opatření.
Cílem je zaměřit se nejprve na oblasti s nejvyšším dopadem na fungování organizace.
Při stanovení priorit je vhodné zohlednit:

- dopad na provoz organizace,
- pravděpodobnost vzniku incidentu,
- rozsah ohrožených aktiv,
- náročnost implementace opatření.

Při stanovení priorit je nutné respektovat princip přiměřenosti.
Zavádění opatření by mělo odpovídat reálným potřebám organizace a jejím kapacitám.
Přehnaně rozsáhlá nebo nepřiměřená opatření mohou vést ke snížení efektivity a obtížné udržitelnosti systému.

Doporučený postup

1. identifikovat nejkritičtější aktiva a služby,
2. určit nejvýznamnější rizika,
3. stanovit opatření pro jejich snížení,
4. rozdělit opatření podle priority (vysoká / střední / nízká),
5. vytvořit plán implementace.

Řízení rizik

Řízení rizik představuje základní princip kybernetické bezpečnosti a výchozí bod pro zavádění bezpečnostních opatření. Cílem řízení rizik je identifikovat a vyhodnotit hrozby, které mohou ovlivnit poskytování služeb, a na tomto základě přijímat přiměřená bezpečnostní opatření.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Tato kapitola popisuje postup, jak řízení rizik zavést v praxi, včetně jednoduchých nástrojů vhodných i pro menší organizace.

Legislativa vyžaduje, aby organizace zaváděly bezpečnostní opatření na základě řízení rizik.

V režimu vyšších povinností je řízení rizik:

- povinné,
- systematické,
- a dokumentované.

V režimu nižších povinností se uplatňuje princip přiměřenosti, přičemž organizace musí být schopna doložit, na základě jakých úvah byla opatření zavedena či nezavedena.

Řízení rizik tedy slouží k tomu, aby organizace identifikovala aktiva a služby, posoudila hrozby a zranitelnosti, vyhodnotila dopady a stanovila odpovídající opatření.

Identifikace aktiv

Prvním krokem je identifikace aktiv, která je potřeba chránit. Aktiva představují vše, co má pro organizaci hodnotu, zejména:

- informační systémy a aplikace,
- data (osobní, provozní, obchodní),
- technickou infrastrukturu,
- služby poskytované zákazníkům nebo veřejnosti.

Důraz je kladen zejména na aktiva, která souvisejí s poskytováním regulované služby.

Organizace vede přehled aktiv, například ve formě tabulky či přehledného seznamu, který bude obsahovat:

- Aktivum (název)
- Popis aktiva
- Vlastníka aktiva (odpovědná osoba)
- Kritičnost

Například:

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Aktivum	Popis	Vlastník	Kritičnost
E-mailový systém	Interní komunikace	IT oddělení	Vysoká
CRM systém	Evidence zákazníků	Obchod	Vysoká
Canva	Zpracování grafických návrhů	PR a marketing	Nízká

Kritičnost aktiva se posuzuje z pohledu:

- dopadu na dostupnost služby,
- dopadu na integritu dat,
- dopadu na důvěrnost informací.

Identifikace rizik

Riziko vzniká kombinací:

- hrozby (co se může stát),
- zranitelnosti (proč se to může stát),
- dopadu (co to způsobí).

Pro každé významné aktivum organizace identifikuje relevantní hrozby (např. kybernetický útok, selhání systému, lidská chyba), zranitelnosti (např. slabé zabezpečení, neaktualizovaný systém) a možné dopady (např. výpadek služby, únik dat).

Rizika jsou evidována v přehledu, který obsahuje alespoň:

- aktivum,
- popis rizika,
- hrozbu a zranitelnost,
- popis dopadu.

Hodnocení rizik (matice rizik)

Rizika jsou hodnocena na základě kombinace:

- pravděpodobnosti výskytu,

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- dopadu na organizaci.

Pro účely tohoto dokumentu je použita jednoduchá tříbodová škála, která odpovídá principu přiměřenosti a je vhodná i pro organizace s omezenými kapacitami.

Pravděpodobnost:

- Nízká – výskyt je nepravděpodobný
- Střední – výskyt je možný
- Vysoká – výskyt je pravděpodobný

Dopad:

- Nízký – omezený dopad bez významného vlivu na poskytované služby
- Střední – částečné omezení provozu nebo služeb
- Vysoký – významný dopad nebo nedostupnost služby

Hodnoticí škála musí být v rámci organizace používána jednotně.

Matice rizik

Dopad/Pravděpodobnost	**Nízká**	**Střední**	**Vysoká**
Nízký	Nízké	Nízké	Střední
Střední	Nízké	Střední	Vysoké
Vysoký	Střední	Vysoké	Kritické

Pro každé identifikované riziko organizace:

- určí pravděpodobnost výskytu,
- určí dopad na organizaci nebo službu,
- přiřadí výslednou úroveň rizika podle matice.

Hodnocení musí být zdokumentováno a opakovatelné.

Na základě vyhodnocení organizace rozhoduje o dalším postupu vůči jednotlivým rizikům.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Organizace může zvolit jeden z následujících přístupů:

- snížení rizika – zavedení bezpečnostních opatření,
- přijetí rizika – vědomé rozhodnutí riziko akceptovat,
- přenos rizika – např. prostřednictvím smluvního vztahu,
- vyhnutí se riziku – změna nebo ukončení činnosti.

Kritéria přijatelnosti rizika

Organizace stanoví, jaké úrovně rizika jsou přijatelné.

Doporučený přístup:

Úroveň rizika	**Přístup**
Kritické	Nepřijatelné – nutné neprodlené řešení
Vysoké	Nepřijatelné – řešit prioritně
Střední	Podmíněně přijatelné – řešit podle kapacit
Nízké	Přijatelné – monitorovat

Kritéria přijatelnosti musí být stanovena předem a uplatňována konzistentně.

Každé riziko musí mít přiřazenu:

- odpovědnou osobu (vlastníka rizika),
- způsob řešení,
- případně termín realizace opatření.

Bez přiřazení odpovědnosti nelze zajistit řízení rizika v praxi.

Výstupy z řízení rizik slouží jako podklad pro výběr a zavádění bezpečnostních opatření, stanovení priorit a plánování bezpečnostních aktivit.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Každé významné riziko by mělo mít odpovídající opatření nebo zdůvodnění jeho nepřijetí.

Dokumentace a aktualizace řízení rizik

Řízení rizik musí být dokumentováno tak, aby bylo možné zpětně doložit přijatá rozhodnutí.
Organizace eviduje alespoň:

- seznam aktiv,
- seznam identifikovaných rizik,
- hodnocení rizik (dopad a pravděpodobnost),
- výslednou úroveň rizika,
- rozhodnutí o způsobu řešení,
- přijatá opatření,
- odpovědnou osobu,
- datum vyhodnocení.

Dokumentace musí být přehledná, aktuální a odpovídat skutečnému stavu.

Musí umožnit doložit jak byla rizika identifikována, jak byla vyhodnocena a jaká rozhodnutí byla přijata.

Rozsah dokumentace a způsob řízení rizik musí odpovídat velikosti a charakteru organizace. Příliš složitý model může být obtížně udržitelný, zatímco příliš zjednodušený model nemusí postačovat pro řízení významných rizik.

Aktualizace řízení rizik

Řízení rizik je průběžný proces a musí být aktualizován zejména:

- při změně systémů, služeb nebo procesů,
- při zavedení nových technologií,
- po bezpečnostním incidentu,
- v pravidelných intervalech.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Spolufinancováno Evropskou unií

Bezpečnostní opatření v praxi

Bezpečnostní opatření představují konkrétní nástroje a procesy, kterými organizace snižuje identifikovaná rizika.

Opatření musí být přiměřená, odůvodněná na základě řízení rizik a udržitelná v praxi.

Tato kapitola poskytuje přehled základních oblastí a minimálních opatření, která by měla být zavedena v každé organizaci.

Přístup „riziko → opatření“

Bezpečnostní opatření nejsou zaváděna izolovaně, ale vždy ve vazbě na identifikovaná rizika. Opatření by vždy mělo odpovídat kritičnosti rizika a mělo by být prakticky proveditelné.

Příklad vazby:

Riziko	**Doporučené opatření**
Slabá hesla	Politika hesel, vícefaktorové ověřování
Phishing	Školení zaměstnanců, ověřovací postupy
Výpadek systému	Zálohování, plán obnovy
Riziko u dodavatele	Smluvní požadavky, kontrola přístupů

Řízení přístupů a identit

Cílem je zajistit, aby k systémům a datům měly přístup pouze oprávněné osoby.

Minimální opatření

- používání jedinečných uživatelských účtů,
- omezení oprávnění na nezbytné minimum (princip „need-to-know“),
- pravidelná kontrola přístupových práv,

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- zavedení vícefaktorového ověřování tam, kde je to možné.

Kontrolní otázky

- Má každý uživatel vlastní účet?
- Jsou přístupy pravidelně kontrolovány?
- Jsou administrátorské účty omezeny?

Správa systémů a zařízení

Cílem je minimalizovat zranitelnosti systémů a zařízení.

Minimální opatření

- pravidelná aktualizace systémů a aplikací,
- evidence používaných zařízení,
- odstranění nebo omezení nepodporovaného software,
- ochrana zařízení proti neoprávněnému přístupu.

Kontrolní otázky

- Jsou systémy pravidelně aktualizovány?
- Existuje přehled zařízení?
- Jsou staré systémy řešeny?

Ochrana dat

Cílem je chránit data před neoprávněným přístupem, ztrátou nebo poškozením. Je potřeba si uvědomit, že datačasto představují nejhodnotnější aktivum organizace.

Minimální opatření

- identifikace citlivých dat,
- omezení přístupu k datům,
- pravidla pro sdílení a ukládání dat,
- zálohování dat.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Kontrolní otázky

- Ví organizace, kde se nacházejí citlivá data?
- Jsou data pravidelně zálohována?
- Je omezen přístup k citlivým informacím?

Lidský faktor

Lidský faktor představuje jednu z nejčastějších příčin incidentů. A bezpečnost každé organizace je jen tak silná, jako je její nejslabší článek.

Minimální opatření

- pravidelná školení zaměstnanců,
- stanovení základních pravidel chování,
- postup pro hlášení podezřelých aktivit.

Kontrolní otázky

- Jsou zaměstnanci školeni alespoň jednou ročně?
- Vědí, jak reagovat na podezřelý e-mail?
- Existuje jednoduchý způsob hlášení incidentu?

Dodavatelé a externí služby

Dodavatelé představují významné bezpečnostní riziko, zejména pokud mají přístup k systémům nebo datům. Incident u dodavatele může ovlivnit i bezpečnost organizace.

Minimální opatření

- identifikace dodavatelů s přístupem k aktivům,
- stanovení bezpečnostních požadavků ve smlouvách,
- omezení přístupů dodavatelů,
- průběžné ověřování dodavatelů.

Kontrolní otázky

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- Ví organizace, kteří dodavatelé mají přístup k systémům?
- Obsahují smlouvy bezpečnostní požadavky?
- Jsou přístupy dodavatelů omezeny?

Kontinuita činností

Cílem je zajistit fungování organizace i v případě incidentu, případně co nejrychlejší navrácení do původního provozu a fungování.

Minimální opatření

- pravidelné zálohování dat,
- plán obnovy provozu,
- testování obnovy dat.

Kontrolní otázky

- Jsou data zálohována?
- Je možné data obnovit?
- Existuje plán pro výpadek systémů?

Řízení incidentů

Cílem je zajistit rychlou a efektivní reakci na incidenty tak, aby incident měl minimální nebo ideálně žádný dopad.

Minimální opatření

- definovaný postup řešení incidentů,
- určení odpovědných osob,
- evidence incidentů.

Kontrolní otázky

- Ví organizace, co dělat při incidentu?
- Je určena odpovědná osoba?
- Jsou incidenty evidovány?

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Spolufinancováno Evropskou unií

Smlouvy a dodavatel

Dodavatelé a externí služby představují významný zdroj rizik, zejména pokud mají přístup k informačním systémům, datům nebo zajišťují klíčové části provozu.

Bezpečnost dodavatele není automaticky zajištěna jeho velikostí, značkou nebo deklarovanou certifikací. Každý dodavatel představuje potenciální vstupní bod do systémů organizace a musí být řízen odpovídajícím způsobem.

Řízení dodavatelů není jednorázová aktivita při uzavření smlouvy, ale průběžný proces zahrnující:

- výběr dodavatele
- smluvní nastavení,
- a následný dohled.

Kdy je dodavatel kritický

Ne každý dodavatel představuje stejné riziko. Organizace by měla identifikovat tzv. kritické dodavatele a dle toho k nim přistupovat.

Kritický dodavatel je typicky takový, který:

- má přístup k interním systémům nebo účtům,
- zpracovává citlivá nebo osobní data,
- zajišťuje klíčovou službu nebo infrastrukturu,
- ovlivňuje dostupnost služeb organizace.

Dodavatele lze rozdělit například:

Typ dodavatele	**Rizikovost**
Bez přístupu k datům a systémům	Nízká
Přístup k omezeným datům	Střední
Přístup k systémům nebo klíčovým datům	Vysoká

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Spolufinancováno Evropskou unií

Bezpečnostní požadavky by měly být odstupňovány podle rizikovosti dodavatele. Není účelné uplatňovat stejné požadavky na všechny dodavatele.

Minimální bezpečnostní požadavky ve smlouvách

Smluvní vztah je základním nástrojem pro řízení bezpečnosti dodavatelů. Každá smlouva s relevantním dodavatelem by měla obsahovat alespoň základní bezpečnostní požadavky.

Minimální požadavky

a) Řízení přístupů

- dodavatel využívá pouze přidělené účty,
- přístupy jsou omezeny na nezbytný rozsah,
- přístupy jsou po ukončení spolupráce odebrány.

b) Ochrana dat

- dodavatel chrání data před neoprávněným přístupem,
- data nejsou používána k jiným účelům,
- data nejsou předávána třetím stranám bez souhlasu.

c) Hlášení incidentů

- dodavatel je povinen oznámit bezpečnostní incident bez zbytečného odkladu,
- incident musí být oznámen definované kontaktní osobě.

d) Bezpečnostní opatření

- dodavatel zavádí odpovídající bezpečnostní opatření,
- dodavatel udržuje systémy aktuální.

e) Subdodavatelé

- zapojení subdodavatelů podléhá souhlasu organizace,
- dodavatel odpovídá za jejich činnost.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

f) Ukončení spolupráce

- vrácení nebo likvidace dat,
- odebrání přístupů,
- ukončení přístupu do systémů.

Ověřování dodavatelů

Bezpečnost dodavatele nelze zajistit pouze smluvně. Formální splnění požadavků (např. certifikace) nemusí znamenat reálnou bezpečnost.

Je nutné ověřovat bezpečnost i praktické fungování.

Před uzavřením smlouvy

- posouzení bezpečnostní úrovně dodavatele,
- ověření referencí,
- ověření vlastnické struktury
- posouzení přístupu k datům a systémům.

V průběhu spolupráce

- kontrola dodržování smluvních podmínek,
- ověřování přístupů,
- komunikace v oblasti bezpečnosti.

Průběžný dohled nad dodavateli

Řízení dodavatelů je kontinuální proces. Je tedy vhodné řízení dodavatelů pravidelně aktualizovat a zlepšovat.

Minimální dohled

- pravidelná kontrola přístupů,
- aktualizace seznamu dodavatelů,
- kontrola plnění bezpečnostních požadavků.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Reakce na incident

- komunikace s dodavatelem,
- vyhodnocení dopadu,
- přijetí nápravných opatření.

Ukončení spolupráce

- odebrání přístupů,
- kontrola odstranění dat,
- aktualizace evidence.

Řízení incidentů

Řízení kybernetických bezpečnostních incidentů představuje jednu z klíčových oblastí kybernetické bezpečnosti. Schopnost organizace reagovat na incident má přímý vliv na rozsah jeho dopadů, délku výpadku služeb i případné finanční a reputační škody.

Cílem řízení incidentů je zajistit, aby organizace byla schopna incident včas rozpoznat, adekvátně na něj reagovat a následně přijmout opatření, která sníží pravděpodobnost jeho opakování.

Postupy pro řízení incidentů by měly být nastaveny tak, aby byly použitelné v praxi. Příliš složité nebo formální procesy mohou vést k tomu, že v reálné situaci nebudou dodrženy.

Cílem není vytvořit rozsáhlou dokumentaci, ale funkční mechanismus, který organizaci umožní reagovat rychle a efektivně.

Kybernetický incident

Kybernetický bezpečnostní incident je událost, která narušuje nebo může narušit důvěrnost, integritu nebo dostupnost informací, systémů nebo služeb.

V praxi se může jednat o široké spektrum situací, od méně závažných událostí, jako je podezřelý e-mail, až po závažné incidenty typu ransomware nebo výpadek klíčového systému.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Spolufinancováno Evropskou unií

Důležité je, aby organizace nepodceňovala ani zdánlivě méně významné události. I drobný incident může být indikátorem závažnějšího problému.

Povinnost detekce a hlášení

Základním předpokladem zvládání incidentů je jejich včasná detekce. Organizace musí mít nastaveny takové procesy, aby bylo možné incident identifikovat a předat k řešení odpovědné osobě.

Součástí tohoto nastavení je také jasně definovaný způsob hlášení. Zaměstnanci by měli vědět, jak postupovat v případě podezřelé situace a komu ji oznámit. Pokud tento mechanismus nefunguje, incidenty často zůstávají neodhaleny nebo jsou řešeny se zpožděním.

V případě významných incidentů vzniká organizaci povinnost hlášení vůči příslušnému orgánu. To předpokládá, že organizace je schopna incident nejen detekovat, ale také vyhodnotit jeho významnost.

Hodnocení významnosti incidentu

Po identifikaci incidentu je nutné určit jeho závažnost. Toto hodnocení slouží jako podklad pro další postup, zejména pro rozhodnutí o eskalaci, zapojení dalších osob nebo nutnosti externího hlášení.

Při hodnocení se zohledňuje zejména dopad incidentu na poskytované služby, rozsah dotčených systémů nebo dat a potenciální následky pro organizaci.

Zjednodušeně lze incidenty rozdělit na:

- méně závažné, které mají omezený dopad a lze je řešit operativně,
- významné, které ovlivňují provoz nebo bezpečnost dat,
- kritické, které mají zásadní dopad na fungování organizace nebo její služby.

Postup při incidentu

Aby byla reakce organizace efektivní, je nutné mít předem definovaný postup. Ten by měl být srozumitelný a použitelný i v situaci, kdy je organizace pod tlakem.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Základní postup zahrnuje několik na sebe navazujících kroků. Nejprve je nutné incident identifikovat a zaznamenat, následně jej oznámit odpovědné osobě. V další fázi je klíčové omezit jeho šíření a minimalizovat dopady. Teprve poté následuje detailnější analýza a obnova provozu.
Důležitou součástí je také dokumentace průběhu řešení, která slouží jak pro interní vyhodnocení, tak pro případné externí požadavky.

Praktický checklist postupu při incidentu

Tento checklist slouží jako orientační pomůcka pro řešení incidentu:

Identifikace a oznámení

- Je incident zaznamenán (čas, systém, popis)?
- Byla informována odpovědná osoba?

Omezení dopadů (containment)

- Bylo zabráněno dalšímu šíření incidentu?
- Byly odpojeny nebo omezeny dotčené systémy/účty?

Základní analýza

- Je znám rozsah incidentu (co je zasaženo)?
- Byly identifikovány možné příčiny?

Obnova

- Byly zahájeny kroky k obnovení provozu?
- Byla ověřena funkčnost systémů?

Dokumentace

- Jsou zaznamenány všechny kroky?
- Jsou evidována přijatá opatření?

Co dělat v prvních 60 minutách

První fáze řešení incidentu je zásadní. V této době se rozhoduje o tom, jak velký dopad bude incident mít.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

V prvních minutách je důležité především rozpoznat, že se jedná o incident, a informovat odpovědnou osobu. Současně je nutné vyvarovat se unáhlených zásahů, které by mohly situaci zhoršit nebo znemožnit následnou analýzu.

Následně by mělo dojít k omezení šíření incidentu, například odpojením napadeného zařízení nebo zablokováním kompromitovaného účtu. Současně je vhodné zaznamenat základní informace o incidentu, jako je čas, dotčený systém nebo popis situace.

V průběhu první hodiny by měla organizace získat základní přehled o rozsahu incidentu a rozhodnout o dalším postupu, včetně případné eskalace nebo nutnosti hlášení.

Zásadní je postupovat systematicky, dokumentovat jednotlivé kroky a zachovat kontrolu nad situací.

Operativní checklist – prvních 60 minut

0–15 minut

- Je potvrzeno, že se jedná o incident?
- Byla informována odpovědná osoba?
- Nedochází k nevratným zásahům (mazání, restart bez evidence)?

15–30 minut

- Bylo omezeno šíření incidentu (odpojení zařízení, blokace účtu)?
- Jsou zaznamenány základní informace (čas, systém, uživatel)?

30–60 minut

- Je znám přibližný rozsah incidentu?
- Bylo rozhodnuto o dalším postupu?
- Je zvážena potřeba eskalace nebo hlášení?

Průběžně

- Jsou dokumentovány provedené kroky?
- Je komunikace řízena a koordinována?

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Následná opatření

Řešením incidentu proces nekončí. Naopak je nutné využít získané zkušenosti k posílení bezpečnosti.

Po každém významnějším incidentu by měla být provedena analýza příčin, která identifikuje, co vedlo k jeho vzniku a zda byla reakce organizace dostatečná.

Na základě této analýzy je vhodné:

- upravit bezpečnostní opatření,
- aktualizovat postupy,
- případně doplnit školení zaměstnanců.

Součástí je také dokumentace incidentu, která umožňuje zpětné vyhodnocení a slouží jako podklad pro další zlepšování.

Řízení a odpovědnosti

Řízení kybernetické bezpečnosti představuje organizační rámec, který určuje, kdo je za jednotlivé oblasti odpovědný a jak jsou bezpečnostní aktivity řízeny.

Jedná se o klíčovou oblast, na kterou legislativa klade důraz zejména ve vztahu k zapojení vrcholného vedení. Kybernetická bezpečnost není pouze technická disciplína, ale součást řízení organizace.

Cílem je zajistit, aby:

- odpovědnosti byly jednoznačně definovány,
- rozhodování bylo řízené a doložitelné,
- a bezpečnost byla integrována do běžného fungování organizace.

Role a odpovědnosti

Pro efektivní řízení kybernetické bezpečnosti je nezbytné jasně definovat role a odpovědnosti.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Spolufinancováno Evropskou unií

Každá organizace by měla stanovit:

- kdo odpovídá za řízení kybernetické bezpečnosti jako celek,
- kdo odpovídá za jednotlivá aktiva nebo oblasti,
- kdo zajišťuje implementaci opatření,
- a kdo provádí kontrolu a dohled.

Nejasné rozdělení odpovědností vede v praxi k tomu, že bezpečnostní opatření nejsou realizována nebo nejsou udržována.

Základní role (obecný přehled):

Role	**Odpovědnost**
Vedení organizace	strategické řízení a rozhodování
Manažer kybernetické bezpečnosti	koordinace a řízení bezpečnosti
Vlastník aktiva	odpovědnost za konkrétní systém/data
IT/provoz	implementace technických opatření

Kontrolní otázky

- Jsou role a odpovědnosti formálně stanoveny?
- Je zřejmé, kdo rozhoduje o rizicích?
- Existuje odpovědnost za jednotlivá aktiva?

Odpovědnost vedení

Vrcholné vedení organizace nese odpovědnost za kybernetickou bezpečnost jako celek.

Tato odpovědnost zahrnuje zejména:

- schvalování bezpečnostní strategie,
- rozhodování o přijatelných rizicích,
- zajištění potřebných zdrojů,
- dohled nad fungováním systému bezpečnosti.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

V praxi to znamená, že kybernetická bezpečnost musí být součástí rozhodovacích procesů na úrovni vedení, nikoli pouze operativní záležitostí IT oddělení.

Typické chyby v praxi

- delegování odpovědnosti bez reálné kontroly,
- nedostatečná informovanost vedení,
- vnímání bezpečnosti jako čistě technické oblasti.

Kontrolní otázky

- Je vedení pravidelně informováno o stavu bezpečnosti?
- Schvaluje vedení klíčová rozhodnutí (např. akceptaci rizik)?
- Jsou vyčleněny odpovídající zdroje?

Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnosti je klíčovou rolí odpovědnou za koordinaci a řízení bezpečnostních aktivit.

Tato role propojuje technickou a organizační rovinu a zajišťuje, že bezpečnostní opatření odpovídají potřebám organizace.

Hlavní odpovědnosti

- řízení systému kybernetické bezpečnosti,
- koordinace implementace opatření,
- komunikace s vedením,
- řízení incidentů a rizik,
- dohled nad dodržováním pravidel.

Manažer kybernetické bezpečnosti by měl mít přístup k vedení organizace, mít dostatečné pravomoci a být zapojen do rozhodovacích procesů.

Bez odpovídajícího postavení je role obtížně vykonatelná.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Kontrolní otázky

- Je role manažera kybernetické bezpečnosti jasně definována?
- Má tato role odpovídající pravomoci?
- Má přímou vazbu na vedení?

Interní vs. externí zajištění

Zajištění role kybernetické bezpečnosti může být realizováno interně nebo externě.

Volba závisí zejména na velikosti organizace, složitosti prostředí a dostupnosti odborných kapacit.

Interní zajištění

Interní pracovník:

- zná prostředí organizace,
- je dostupný pro operativní řešení,
- může dlouhodobě rozvíjet bezpečnostní systém.

Nevýhodou mohou být vyšší náklady a omezená dostupnost odborníků.

Externí zajištění

Externí zajištění:

- přináší zkušenosti z různých prostředí,
- umožňuje flexibilní rozsah služeb,
- může být nákladově efektivní.

Nevýhodou může být nižší znalost interního prostředí a omezená dostupnost.

V praxi se často využívá kombinace kdy externí odborník nastaví systém a interní pracovník jej dále rozvíjí a udržuje.

Kontrolní otázky

- Je jasně definováno, kdo roli vykonává?

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

- Má tato osoba dostatečné kompetence?
- Je zajištěna zastupitelnost?

Bez jasně definovaných odpovědností nelze efektivně řídit kybernetickou bezpečnost. Cílem není vytvořit složitou organizační strukturu, ale zajistit, aby bylo vždy zřejmé:

- kdo rozhoduje,
- kdo provádí,
- a kdo kontroluje.

Implementace a zlepšování

Kybernetická bezpečnost není jednorázový projekt, ale průběžný proces. Zavedení bezpečnostních opatření je pouze prvním krokem, klíčová je jejich dlouhodobá udržitelnost a postupné zlepšování.

Tato kapitola vychází z principu cyklického řízení (plan–do–check–act), který je přeložen do praktického postupu vhodného pro běžné organizace.

Cílem je zajistit, aby:

- bezpečnostní opatření byla skutečně implementována,
- jejich účinnost byla pravidelně vyhodnocována,
- a systém se postupně rozvíjel.

Zavedení systému bezpečnosti

Zavedení systému kybernetické bezpečnosti znamená převést identifikovaná rizika a navržená opatření do praxe. Nejde pouze o vytvoření dokumentace, ale o skutečné nastavení procesů a odpovědností.

Častou chybou je zaměření na tvorbu dokumentů bez reálného zavedení opatření. Bezpečnostní opatření musí být nejen popsána, ale i skutečně používána.

Doporučený postup

Zavedení systému probíhá typicky v několika krocích:

1. stanovení rozsahu (co je zahrnuto),

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

2. definování rolí a odpovědností,
3. identifikace rizik,
4. výběr bezpečnostních opatření,
5. jejich implementace do praxe.

Kontrolní otázky

- Jsou opatření skutečně zavedená, nebo pouze zdokumentovaná?
- Jsou role a odpovědnosti funkční?
- Odpovídá rozsah systému realitě organizace?

Průběžné hodnocení

Po zavedení opatření je nutné pravidelně vyhodnocovat jejich účinnost.

Cílem je zjistit, zda opatření fungují podle očekávání, odpovídají aktuálním rizikům a nejsou obcházená nebo nefunkční.

Způsoby hodnocení

- kontrola dodržování pravidel,
- vyhodnocení incidentů,
- zpětná vazba od zaměstnanců,
- kontrola nastavení systémů.

Kontrolní otázky

- Jsou opatření pravidelně kontrolována?
- Jsou zjištěné nedostatky řešeny?
- Odpovídají opatření aktuálním rizikům?

Audit a kontrola

Audit představuje systematické ověření toho, zda je systém kybernetické bezpečnosti nastaven správně a funguje v praxi.

V režimu vyšších povinností je audit povinný a provádí se v pravidelných intervalech.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Typy kontrol

- interní kontrola (vlastní ověření),
- externí audit (nezávislé posouzení),
- tematické kontroly (např. přístupy, dodavatelé).

Cílem auditu je identifikace nedostatků, ověření souladu s požadavky a následné doporučení pro zlepšení.

Kontrolní otázky

- Probíhá pravidelná kontrola systému?
- Jsou výsledky auditu dokumentovány?
- Jsou přijímána nápravná opatření?

Zlepšování

Zlepšování je kontinuální proces, jehož cílem je postupné zvyšování úrovně kybernetické bezpečnosti.
Cílem není dosáhnout „dokonalého stavu“, ale zajistit, aby se bezpečnostní úroveň organizace postupně zvyšovala a reagovala na aktuální vývoj.

Impulsem ke zlepšení mohou být výsledky auditů, bezpečnostní incidenty, změny v organizaci nebo technologiích či nové hrozby.

Postup zlepšování

1. identifikace nedostatku nebo příležitosti,
2. návrh opatření,
3. implementace,
4. ověření účinnosti.

Kontrolní otázky

- Jsou identifikované nedostatky skutečně řešeny?
- Dochází k aktualizaci opatření?
- Reaguje organizace na nové hrozby?

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Shrnutí principu

Systém kybernetické bezpečnosti by měl fungovat jako cyklus:

- zavedení opatření,
- jejich ověření,
- a následné zlepšení.

Tento cyklus zajišťuje, že bezpečnost není statická, ale přizpůsobuje se vývoji organizace i hrozeb.

Praktické nástroje a šablony

Tato kapitola obsahuje základní nástroje a šablony, které mohou organizace přímo využít při zavádění a řízení kybernetické bezpečnosti.

Cílem je poskytnout jednoduché a použitelné pomůcky, které usnadní implementaci požadavků, sníží administrativní náročnost a pomohou zajistit konzistentní postup.

Uvedené nástroje představují minimální základ a mohou být upraveny podle potřeb organizace.

Uvedené nástroje slouží jako základní rámec.
Každá organizace by je měla přizpůsobit svým potřebám, velikosti a úrovni rizik.

Důležitější než forma je jejich skutečné využívání v praxi.

Matice řízení rizik (vzor)

Organizace může evidovat rizika například v následující tabulce:

Aktivum	**Riziko**	**Dopad**	**Pravděpodobnost**	**Úroveň rizika**	**Opatření**	**Odpovědnost**	**Termín**
E-mail	*Phishing*	*Vysoký*	*Střední*	*Vysoké*	*Školení, 2FA*	*IT*	*30. 6.*

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Spolufinancováno Evropskou unií

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

T A
Č R

Pokyny k použití

- evidovat pouze relevantní (významná) rizika,
- pravidelně aktualizovat,
- přiřadit odpovědnost za každé riziko.

Checklist minimálních opatření

Otázka	Ano/Ne/Částečně
Technická opatření	
Jsou systémy pravidelně aktualizovány?	
Je používán antivirový nebo jiný ochranný software?	
Jsou přístupy zabezpečeny (hesla, 2FA)?	
Organizační opatření	
Jsou definovány role a odpovědnosti?	
Existuje základní bezpečnostní dokumentace?	
Probíhá školení zaměstnanců?	
Provozní opatření	
Jsou data pravidelně zálohována?	
Existuje postup pro řešení incidentů?	
Jsou řízeni dodavatelé?	

Incident response checklist

Otázka	Ano/Ne/Částečně
Je incident zaznamenán?	

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Byla informována odpovědná osoba?	
Bylo zabráněno dalšímu šíření?	
Je znám rozsah incidentu?	
Probíhá obnova provozu?	
Jsou dokumentovány kroky?	

Dodavatelský checklist

Checklist pro řízení dodavatelů a smluv.

Otázka	**Ano/Ne**
Před uzavřením smlouvy	
Má dodavatel přístup k datům nebo systémům?	
Byla posouzena jeho bezpečnostní úroveň?	
Smlouva obsahuje	
Požadavky na ochranu dat?	
Povinnost hlášení incidentů?	
Pravidla pro přístupy?	
Podmínky pro subdodavatele?	
V průběhu spolupráce	
Jsou přístupy dodavatele aktuální a omezené?	
Je dodavatel pravidelně vyhodnocován?	
Je komunikace dostatečná?	

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Spolufinancováno Evropskou unií

Přílohy

Desatero bezpečného chování

Následující doporučení představují základní pravidla bezpečného chování v digitálním prostředí. Jsou určena všem zaměstnancům organizace a jejich dodržování významně snižuje riziko kybernetických incidentů.

1. Používejte silná a jedinečná hesla

Používejte hesla, která nejsou snadno odhadnutelná. Vhodná je kombinace velkých a malých písmen, čísel a speciálních znaků, případně delší přístupové fráze.

Pro každý účet používejte jiné heslo.

2. Aktivujte dvoufázové ověřování (2FA)

Dvoufázové ověřování zvyšuje úroveň zabezpečení účtů. Pokud je tato možnost dostupná, aktivujte ji nejen u pracovních, ale i soukromých účtů.

3. Buďte opatrní při práci s odkazy a přílohami

Neotevírejte odkazy ani přílohy z neznámých nebo podezřelých zdrojů. Před kliknutím si vždy ověřte odesílatele a adresu odkazu.

4. Chraňte osobní a citlivé údaje

Nikdy nesdílejte citlivé informace (např. přístupové údaje, osobní data, bankovní informace) na veřejných nebo neověřených platformách.

5. Udržujte software aktuální

Pravidelně aktualizujte operační systém i aplikace. Aktualizace často obsahují opravy bezpečnostních zranitelností.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

6. Vyhněte se používání veřejných Wi-Fi sítí

Veřejné Wi-Fi sítě mohou být nezabezpečené. Pokud je nutné je použít, doporučuje se využít zabezpečené připojení (např. VPN).

7. Zamykejte zařízení při odchodu

Při opuštění pracovního místa vždy uzamkněte počítač nebo jiné zařízení. Tím zabráníte neoprávněnému přístupu k datům.

8. Průběžně se vzdělávejte

Kybernetické hrozby se neustále vyvíjejí. Sledujte aktuální informace a účastněte se školení v oblasti kybernetické bezpečnosti.

9. Buďte obezřetní vůči podvodným aktivitám

Dávejte si pozor na podvodné e-maily, telefonáty nebo webové stránky. Důvěryhodné instituce po vás nebudou požadovat citlivé údaje tímto způsobem.

10. Dodržujte interní bezpečnostní pravidla

Seznamte se s interními zásadami kybernetické bezpečnosti a dodržujte je. Kybernetická bezpečnost je společná odpovědnost všech zaměstnanců.

Slovníček pojmů a zkratek

Tento slovníček obsahuje vybrané pojmy a zkratky používané v oblasti kybernetické bezpečnosti a v tomto dokumentu.

Obecné pojmy

CIA (Confidentiality, Integrity, Availability)

Základní principy bezpečnosti informací: důvěrnost, integrita a dostupnost.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

ICT / IKT (Information and Communication Technologies)

Informační a komunikační technologie.

KB (Kybernetická bezpečnost)

Soubor opatření sloužících k ochraně informačních systémů, sítí a dat.

MSP / SME (Small and Medium-sized Enterprises)

Malé a střední podniky.

State-of-the-Art (SotA)

Současný stav poznání a praxe v dané oblasti.

Organizace a instituce

ENISA (European Union Agency for Cybersecurity)

Agentura Evropské unie pro kybernetickou bezpečnost.

Národní autorita kybernetické bezpečnosti

Orgán odpovědný za regulaci a dohled v oblasti kybernetické bezpečnosti na národní úrovni.

ECCC (European Cybersecurity Competence Centre)

Evropské centrum kompetencí pro kybernetickou bezpečnost.

Právní rámec

NIS2

Směrnice Evropské unie zaměřená na zajištění vysoké úrovně kybernetické bezpečnosti.

Zákon o kybernetické bezpečnosti (ZKB/ZoKB)

Národní právní předpis upravující povinnosti organizací v oblasti kybernetické bezpečnosti.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

Cyber Resilience Act (CRA)

Evropské nařízení zaměřené na bezpečnost digitálních produktů.

Cybersecurity Act (CSA)

Nařízení EU upravující certifikaci kybernetické bezpečnosti a roli ENISA.

Další pojmy

Incident

Událost, která narušuje nebo ohrožuje bezpečnost informací nebo služeb.

Riziko

Kombinace pravděpodobnosti hrozby a jejího dopadu.

Zranitelnost

Slabé místo, které může být zneužito hrozbou.

Hrozba

Událost nebo činnost, která může způsobit škodu.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.


Spolufinancováno Evropskou unií. Uvedené názory a stanoviska vyjadřují pouze názory autora(ů) a nemusí nutně odrážet názory Evropské unie ani Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost. Evropská unie ani poskytovatel dotace nenesou za tyto názory odpovědnost.

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.