BEARCLAVE

# Report z analýzy

Soulad Microsoft 365 a Azure se zákonem o kybernetické bezpečnosti — režim vyšších povinností

| | |
|---|---|
| Verze | 1.0 |
| Zpracoval | Bearclave s.r.o. |
| Klasifikace | Veřejné — vzorový dokument |

*Bearclave s.r.o., Třešňová 916/16, Přímětice, 669 04 Znojmo*
*IČO 30007534 · DIČ CZ30007534 · zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 153837*
*info@bearclave.cz · bearclave.cz*

# 1. Manažerské shrnutí

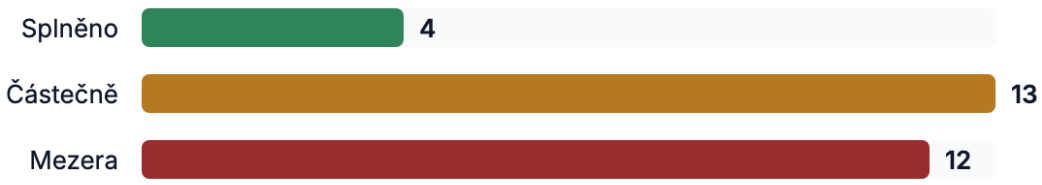
Organizace je poskytovatelem regulované služby v režimu vyšších povinností, protože provozuje vodovod sloužící veřejné potřebě (služba 10.1 přílohy vyhlášky č. 408/2025 Sb.) a je velkým podnikem. Bezpečnostní opatření proto zavádí podle § 14 odst. 1 zákona č. 264/2025 Sb. a vyhlášky č. 409/2025 Sb., ne podle vyhlášky č. 410/2025 Sb. pro nižší povinnosti, a incidenty hlásí Úřadu podle § 15 odst. 1 a § 16 zákona.

| **Vyšší** | **29** | **4** | **12** |
|---|---|---|---|
| režim povinností podle přílohy vyhlášky 408/2025, služba 10.1 | ustanovení namapovaných na Microsoft 365 a Azure | z nich je splněno | mezer, z toho 1 kritická |

Z 29 namapovaných ustanovení je 4 splněno, 13 částečně a u 12 chybí požadované nastavení. Dohromady jde o 12 mezer. Kritická je jediná: čtyři sdílené účty dispečinku se přihlašují jen heslem, dva z nich i mimo síť dispečinku.

Vysokou prioritu má 6 mezer, mezi nimi chybějící cesta od incidentu k prvotnímu hlášení do 24 hodin a uchovávání záznamů 90 dní místo 18 měsíců. V pořádku je síť a šifrování portálu, centrální řízení oprávnění a správa portálu s vícefaktorovou autentizací. Doporučujeme začít sdílenými účty a retencí záznamů, u retence znamená každý den odkladu nevratně ztracené záznamy.

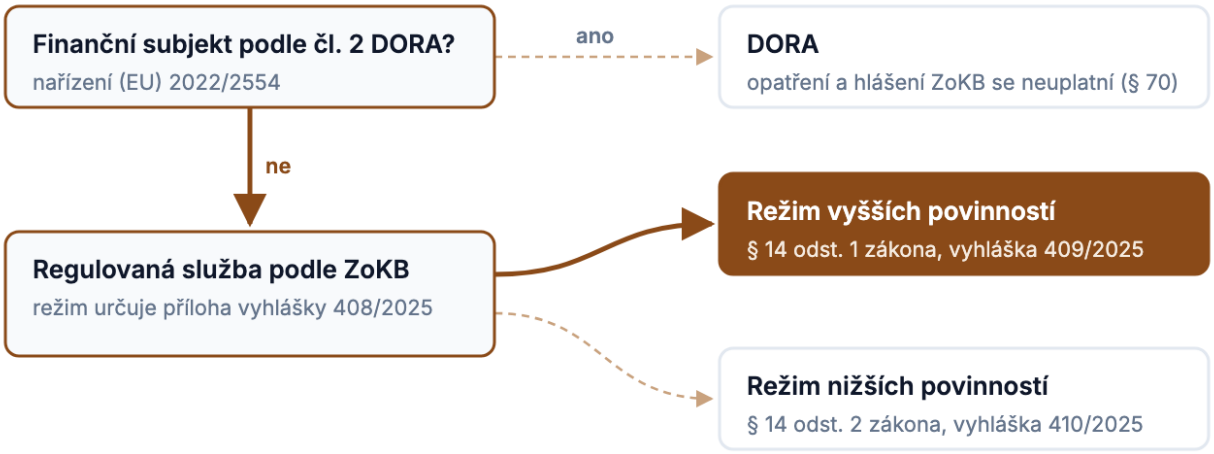
*Stav 29 namapovaných ustanovení*



# 2. Režim a rozsah

## 2.1 Určení režimu

*Cesta k režimu organizace*




*Režim vyplývá z rozhodnutí o registraci a z vyhodnocení organizace, analýza ho přebírá a neposuzuje*

| Regulovaná služba | Podmínka | Režim | Měří se proti | Hlášení |
|---|---|---|---|---|
| 10.1 Provozování vodovodu sloužícího veřejné potřebě | příjmy ze služby alespoň 5 % obratu, velký podnik | Vyšší povinnosti | zákon § 14 odst. 1, vyhláška 409/2025 | § 15 odst. 1 a § 16 zákona, Úřad |
| Pro srovnání: tatáž služba u středního podniku | příjmy ze služby alespoň 5 % obratu, střední podnik | Nižší povinnosti | zákon § 14 odst. 2, vyhláška 410/2025 | § 15 odst. 2 a § 16 zákona, Národní CERT |

**příloha, bod 10.1 Provozování vodovodu sloužícího veřejné potřebě, vyhlášky č. 408/2025 Sb.**

Provozovatel vodovodu podle zákona o vodovodech a kanalizacích, jehož příjmy spojené s touto službou tvořily alespoň 5 % jeho obratu za poslední účetní období, je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je velkým podnikem, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.

**§ 8 odst. 1 a 2 zákona č. 264/2025 Sb.**

(1) V režimu vyšších povinností je poskytovatel regulované služby, který z důvodu své velikosti, počtu uživatelů, geografického rozšíření služby, dopadu na fungování odvětví nebo jiného poskytovatele regulované služby nebo rizikovosti provozu, je značně ekonomicky, společensky nebo bezpečnostně významný pro Českou republiku. V režimu nižších povinností je poskytovatel regulované služby, který není v režimu vyšších povinností podle věty první.
(2) Rozdělení poskytovatelů podle poskytovaných regulovaných služeb do režimů uvedených v odstavci 1 stanoví Úřad vyhláškou.

## 2.2 Prostředí

| Prostředí | Hodnota |
|---|---|
| Microsoft 365 | 380 uživatelů, licence E3 (Entra ID P1, Intune, Defender for Endpoint Plan 1) |
| Azure | tři předplatná: zákaznický portál, sdílené služby, vývoj |
| Zákaznický portál | App Service za Application Gateway s WAF, Azure SQL Database, úložiště dokumentů, Key Vault, dva servery integrace s Defender for Servers Plan 2 |
| Dohled | Microsoft Sentinel, nasazený externím dodavatelem, bez smlouvy na dohled |
| Přístup analýzy | jen čtení, bez zásahu do provozu, záznamy za 90 dní |

*Stanovený rozsah podle § 12 zákona, jak ho předala organizace*

| Aktivum v rozsahu | Kde běží | Co z něj analýza pokrývá |
|---|---|---|
| Dispečerské řízení | vlastní servery | jen účty dispečerů, schránka poruch a Teams pohotovosti |
| Zákaznický portál | Azure | celou službu kromě kódu aplikace, který vyvíjí dodavatel |
| Identita a pošta | Microsoft 365 | účty, role, ověřování, hosty a aplikace třetích stran |

## 2.3 Co analýza není

- Není to právní posouzení, výklad předpisů i určení režimu patří právníkovi.
- Nepokrývá organizační povinnosti, aktiva mimo cloud ani kód portálu.
- Mapuje ustanovení se zjištěním v prostředí, ne každé písmeno vyhlášky.
- Nezaručuje soulad se zákonem jako celek, ani po odstranění všech mezer.

# 3. Relevantní ustanovení

| Zákon | Opatření | Vyhláška | Odraz v M365 a Azure |
|---|---|---|---|
| a) 1 | Systém řízení bezpečnosti informací | § 3 | Žádný |
| a) 2 | Požadavky na vrcholné vedení | § 4 | Žádný |
| a) 3 | Stanovení bezpečnostních rolí | § 5 | Žádný |
| a) 4 | Řízení bezpečnostní politiky a bezpečnostní dokumentace | § 6 | Žádný |
| a) 5 | Řízení aktiv | § 7 | Částečný |
| a) 6 | Řízení rizik | § 8 | Žádný |
| a) 7 | Řízení dodavatelů | § 9 | Částečný |
| a) 8 | Bezpečnost lidských zdrojů | § 10 | Žádný |
| a) 9 | Řízení změn | § 11 | Částečný |
| a) 10 | Akvizice, vývoj a údržba | § 12 | Částečný |
| a) 11 | Řízení přístupu | § 13 | Přímý |
| a) 12 | Zvládání kybernetických bezpečnostních událostí a incidentů | § 14 | Částečný |
| a) 13 | Řízení kontinuity činností | § 15 | Žádný |
| a) 14 | Provádění auditu kybernetické bezpečnosti | § 16 | Žádný |
| b) 1 | Fyzická bezpečnost | § 17 | Žádný |
| b) 2 | Bezpečnost komunikačních sítí | § 18 | Částečný |
| b) 3 | Správa a ověřování identit | § 19 | Přímý |
| b) 4 | Řízení přístupových práv a oprávnění | § 20 | Přímý |
| b) 5 | Detekce kybernetických bezpečnostních událostí | § 21 | Přímý |
| b) 6 | Zaznamenávání událostí | § 22 | Přímý |
| b) 7 | Vyhodnocování kybernetických bezpečnostních událostí | § 23 | Přímý |
| b) 8 | Aplikační bezpečnost | § 24 | Částečný |
| b) 9 | Kryptografické algoritmy | § 25 | Přímý |
| b) 10 | Zajišťování dostupnosti regulované služby | § 26 | Přímý |
| b) 11 | Zabezpečení průmyslových, řídících a obdobných specifických technických aktiv | § 27 | Žádný |

> 25 opatření podle § 14 odst. 1 zákona, a) 11 = písm. a) bod 11. Odraz přímý (8): nastavuje se v cloudu, částečný (7): jen část, žádný (10): organizační nebo fyzické opatření.

# 4. Mapování

*§ = vyhláška č. 409/2025 Sb.; splněno: vše v pořádku, částečně: něco chybí, mezera: v cloudu chybí vše*

| Opatření | § | Stav | Mezery |
|---|---|---|---|
| Řízení aktiv | zákon § 12, § 7 | Částečně | M-01, M-02 |
| Řízení dodavatelů | § 9 | Mezera | M-03, M-04 |
| Řízení změn | § 11 | Částečně | — |
| Akvizice, vývoj a údržba | § 12 | Částečně | — |
| Řízení přístupu | § 13 | Částečně | M-03 až M-06, M-08 |
| Zvládání událostí a incidentů | § 14 | Mezera | M-07 |
| Hlášení incidentů | zákon § 15 a 16 | Mezera | M-07 |
| Bezpečnost komunikačních sítí | § 18 | Splněno | — |
| Správa a ověřování identit | § 19 | Částečně | M-08 |
| Řízení přístupových práv a oprávnění | § 20 | Splněno | — |
| Detekce událostí | § 21 | Částečně | M-09 |
| Zaznamenávání událostí | § 22 | Částečně | M-09, M-10 |
| Vyhodnocování událostí | § 23 | Částečně | M-07 |
| Aplikační bezpečnost | § 24 | Částečně | M-09 |
| Kryptografické algoritmy | § 25 | Částečně | M-09 |
| Dostupnost regulované služby | § 26 | Částečně | M-11, M-12 |

> Stav hodnotí nastavení Microsoft 365 a Azure v té části stanoveného rozsahu, která v nich běží. Kde cloud k organizační povinnosti dodá jen podklad, překlad to výslovně uvádí.

## 4.1 Řízení aktiv — zákon § 12 a § 7

### § 12 odst. 3 — evidence aktiv ve stanoveném rozsahu podle zákona

> **§ 12 odst. 3 zákona č. 264/2025 Sb.**
>
> (3) Poskytovatel regulované služby eviduje aktiva, která jsou součástí stanoveného rozsahu, a primární aktiva, která byla ze stanoveného rozsahu vyjmuta, včetně důvodů jejich vyjmutí.

**Překlad do Microsoft 365 a Azure**

- Tag stanoveného rozsahu vynucený Azure Policy, export jako podklad evidence aktiv

| Zjištěno | Stav | Mezera |
|---|---|---|
| Evidence aktiv organizace nezná 2 z 9 prostředků portálu, nové vznikají bez tagu. | Částečně | M-02 |

### § 7 písm. f) — vazby mezi aktivy

> **§ 7 písm. f) vyhlášky č. 409/2025 Sb.**
>
> Povinná osoba v návaznosti na stanovení rozsahu řízení kybernetické bezpečnosti podle § 12 zákona
> ...
> f) určuje a eviduje vazby mezi aktivy, která mají vliv na bezpečnost regulované služby,

**Překlad do Microsoft 365 a Azure**

- Tagy služby a garanta aktiva na prostředcích Azure, vynucené Azure Policy
- Export z Azure Resource Graph jako podklad evidence vazeb, kterou vede organizace

| Zjištěno | Stav | Mezera |
|---|---|---|
| Úložiště a Key Vault portálu leží ve sdílených službách bez tagů. Evidence aktiv vede portál bez vazby na ně. | Částečně | M-02 |

### § 7 písm. h) body 3 a 4 — klasifikace informací a označování aktiv

> **§ 7 písm. h) body 3 a 4 vyhlášky č. 409/2025 Sb.**
>
> Povinná osoba v návaznosti na stanovení rozsahu řízení kybernetické bezpečnosti podle § 12 zákona
> ...
> h) pro jednotlivé úrovně aktiv podle písmene b) stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, integrity a dostupnosti, která obsahují alespoň
> ...
> 3. pravidla pro klasifikaci informací,
> 4. pravidla pro označování aktiv,

**Překlad do Microsoft 365 a Azure**

- Popisky citlivosti v Microsoft Purview podle úrovní aktiv, s E3 ruční označování
- Pravidla klasifikace a označování stanoví organizace, Microsoft 365 je jen zavádí

| Zjištěno | Stav | Mezera |
|---|---|---|
| Pravidla klasifikace ani označování nejsou stanovená a Microsoft 365 nemá žádné popisky citlivosti. | **Mezera** | M-01 |

## 4.2 Řízení dodavatelů — § 9

### § 9 odst. 1 písm. c) — rizika spojená s dodavateli

> **§ 9 odst. 1 písm. c) vyhlášky č. 409/2025 Sb.**
>
> (1) Povinná osoba při řízení dodavatelů
> ...
> c) řídí rizika spojená s dodavateli,

**Překlad do Microsoft 365 a Azure**

- Aplikace dodavatelů jen s oprávněním ke schránkám, které potřebují
- Delegovaný přístup partnera přes GDAP jen s nutnými rolemi a na dobu smlouvy
- Export přístupů dodavatelů z Entra ID jako podklad hodnocení rizik organizace

| Zjištěno | Stav | Mezera |
|---|---|---|
| 3 aplikace dodavatelů smějí číst všechny schránky a partner má delegovanou roli globálního správce. Rizika dodavatelů mimo cloud analýza neposuzovala. | **Mezera** | M-03, M-04 |

## 4.3 Řízení změn — § 11

### § 11 odst. 2 písm. a) — dokumentace řízení významných změn

> **§ 11 odst. 2 písm. a) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba u významných změn
> a) dokumentuje jejich řízení,

**Překlad do Microsoft 365 a Azure**

- Nasazení portálu přes pipeline se schválením a historií jako doklad řízení změn
- Určení významných změn a jejich dokumentace mimo portál jsou organizační
- Záznam změn v Sentinelu ukáže, co se změnilo, ne jak se změna řídila

| Zjištěno | Stav | Mezera |
|---|---|---|
| Portál se nasazuje jen přes pipeline Azure DevOps se schválením a historií. Změny Microsoft 365 a Entra ID se jen zaznamenávají. | Částečně | — |

## 4.4 Akvizice, vývoj a údržba — § 12

### § 12 odst. 2 písm. a) — autentizace u pořizovaných a vyvíjených aktiv

> **§ 12 odst. 2 písm. a) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba zajistí při provedení akvizice nebo vývoje technického aktiva
> a) využívajícího autentizační mechanismus, zejména za účelem ověření identity uživatelů nebo administrátorů, plnění požadavků podle § 19 odst. 2,

**Překlad do Microsoft 365 a Azure**

- Správa portálu přes Entra ID s vícefaktorovou autentizací

| Zjištěno | Stav | Mezera |
|---|---|---|
| Správa portálu přijímá jen účty Entra ID s vícefaktorovou autentizací. Přihlášení zákazníků je v kódu aplikace, který analýza nepokrývá; zda se na ně vztahuje § 19 odst. 2, posoudí organizace s právníkem. | Částečně | — |

## 4.5 Řízení přístupu — § 13

### § 13 odst. 2 písm. b) — nezbytná oprávnění a oddělené účty

> **§ 13 odst. 2 písm. b) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba dále při řízení přístupu k aktivům
>
> ...
>
> b) přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu práce a jedinečný identifikátor daného typu účtu, přičemž odděluje uživatelské a administrátorské účty jedné osoby,

**Překlad do Microsoft 365 a Azure**

- Úzké role místo globálního správce, v PIM jen s aktivací na čas (Entra ID P2)
- Samostatný administrátorský účet bez pošty pro každého správce
- Osobní účet pro každého dispečera, sdílená schránka přes delegaci

| Zjištěno | Stav | Mezera |
|---|---|---|
| 17 trvalých přiřazení privilegovaných rolí, z toho 6 globálních správců. 4 správci nemají oddělený účet, 4 sdílené účty dispečinku nepatří konkrétní osobě. | Částečně | M-05, M-08 |

### § 13 odst. 2 písm. c) — účty technických aktiv

> **§ 13 odst. 2 písm. c) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba dále při řízení přístupu k aktivům
>
> ...
>
> c) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,

**Překlad do Microsoft 365 a Azure**

- Přístup aplikací k poště omezený RBAC pro aplikace v Exchange Online
- Souhlas uživatelů s aplikacemi vypnutý, souhlas uděluje správce

| Zjištěno | Stav | Mezera |
|---|---|---|
| Portál používá spravované identity s úzkou rolí. 11 aplikací třetích stran má oprávnění k poště, 3 ke všem schránkám, 5 schválili sami uživatelé. | Částečně | M-03 |

## § 13 odst. 2 písm. h) — pravidelný přezkum oprávnění

> **§ 13 odst. 2 písm. h) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba dále při řízení přístupu k aktivům
>
> ...
>
> h) provádí pravidelné přezkoumání veškerých přístupových práv a oprávnění včetně rozdělení do skupin a rolí,

**Překlad do Microsoft 365 a Azure**

- Čtvrtletní přezkumy přístupu (Entra ID P2 nebo Entra ID Governance)
- Přezkum privilegovaných rolí v PIM (Entra ID P2)
- Do nasazení licencí čtvrtletní přezkum exportem, potvrzený vedoucími

| Zjištěno | Stav | Mezera |
|---|---|---|
| Přístupová práva nikdo nepřezkoumává. Organizace má Entra ID P1, přezkumy přístupu v ní nejsou. | **Mezera** | M-06 |

## § 13 odst. 2 písm. i) — změna práv při změně pozice

> **§ 13 odst. 2 písm. i) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba dále při řízení přístupu k aktivům
>
> ...
>
> i) zajistí bezodkladné odebrání nebo změnu přístupových práv a oprávnění při změně pozice nebo zařazení na základě skupin a rolí,

**Překlad do Microsoft 365 a Azure**

- Dynamické skupiny podle pozice nebo oddělení, role jen přes skupiny
- Při přeřazení odebrat statické skupiny a role podle seznamu z personální agendy

| Zjištěno | Stav | Mezera |
|---|---|---|
| Při změně pozice role a statické skupiny zůstávají, nikdo je neodebírá. | **Mezera** | M-06 |

### § 13 odst. 2 písm. j) — deaktivace při ukončení vztahu

> **§ 13 odst. 2 písm. j) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba dále při řízení přístupu k aktivům
>
> ...
>
> j) zajistí deaktivaci účtů a bezodkladné odebrání nebo změnu přístupových práv a oprávnění při ukončení nebo změně smluvního vztahu, na základě kterého došlo ke zřízení přístupu k aktivům,

**Překlad do Microsoft 365 a Azure**

- Blokace účtu a odvolání relací v den odchodu
- Hosté dodavatelů s vlastníkem v organizaci a přezkumem trvání smlouvy

| Zjištěno | Stav | Mezera |
|---|---|---|
| Odcházejícím se účet blokuje v den odchodu. 2 z 5 hostů dodavatele jsou přes 6 měsíců neaktivní a nikdo neověřil, zda jejich smluvní vztah trvá. | Částečně | M-04 |

## 4.6 Zvládání událostí a incidentů — § 14

### § 14 odst. 1 písm. c) a g) — odpovědnosti a posouzení událostí

> **§ 14 odst. 1 písm. c) a g) vyhlášky č. 409/2025 Sb.**
>
> (1) Povinná osoba při zvládání kybernetických bezpečnostních událostí a incidentů
>
> ...
>
> c) přidělí odpovědnosti pro
> 1. detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí a
> 2. koordinaci a zvládání kybernetických bezpečnostních incidentů,
>
> ...
>
> g) zajistí posuzování kybernetických bezpečnostních událostí, při kterých musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty,

**Překlad do Microsoft 365 a Azure**

- Automatizační pravidlo v Sentinelu přiřadí incident řešiteli podle závažnosti
- Úkol posoudit, zda jde o kybernetický bezpečnostní incident, a značka s výsledkem
- Odpovědnosti a pravidla posouzení určí organizace, Sentinel je vynutí a doloží

| Zjištěno | Stav | Mezera |
|---|---|---|
| Z 212 incidentů za 90 dní je 64 % bez řešitele a nikdo je neposoudil. Klasifikace v Sentinelu neříká, zda jde o incident podle zákona. | Mezera | M-07 |

## 4.7 Hlášení incidentů — zákon § 15 a 16

### § 15 odst. 1 — okruh hlášených incidentů podle zákona

> **§ 15 odst. 1 zákona č. 264/2025 Sb.**
>
> (1) Poskytovatel regulované služby v režimu vyšších povinností je povinen hlásit Úřadu postupem podle § 16 kybernetické bezpečnostní incidenty, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění.

**Překlad do Microsoft 365 a Azure**

- Watchlist aktiv v rozsahu, incident nad nimi dostane úkol posoudit hlášení
- Posoudí se tři podmínky zákona, významnost dopadu se neposuzuje
- Výsledek posouzení a jeho důvod jako komentář v incidentu

| Zjištěno | Stav | Mezera |
|---|---|---|
| Z incidentu nejde poznat, zda se projevil ve stanoveném rozsahu, ani kdo a jak posoudil, zda podléhá hlášení. | **Mezera** | M-07 |

### § 16 odst. 1 — prvotní hlášení do 24 hodin podle zákona

> **§ 16 odst. 1 zákona č. 264/2025 Sb.**
>
> (1) Poskytovatel regulované služby bez zbytečného odkladu, nejpozději do 24 hodin po zjištění kybernetického bezpečnostního incidentu, předloží prvotní hlášení, v němž uvede své identifikační údaje, základní údaje o kybernetickém bezpečnostním incidentu, a zda se domnívá, že byl kybernetický bezpečnostní incident způsoben nezákonným zásahem nebo že by mohl mít přeshraniční dopad.

**Překlad do Microsoft 365 a Azure**

- Upozornění do Teams a na telefon pohotovosti, eskalace po 2 hodinách bez převzetí
- Hlídání lhůty 24 hodin od zjištění, hlášení samo přes Portál Úřadu

| Zjištěno | Stav | Mezera |
|---|---|---|
| Upozornění chodí jen e-mailem, který mimo pracovní dobu nikdo nečte. První zásah u závažných incidentů trvá v mediánu 31 hodin. | **Mezera** | M-07 |

## § 16 odst. 3 písm. a) a c) — oznámení a závěrečná zpráva podle zákona

**§ 16 odst. 3 písm. a) a c) zákona č. 264/2025 Sb.**

(3) V případě hlášení kybernetického bezpečnostního incidentu s významným dopadem na poskytování regulované služby podle § 15 odst. 2 nebo na kybernetický prostor státu podle odstavce 2 poskytovatel regulované služby dále předloží

a) bez zbytečného odkladu, nejpozději do 72 hodin po zjištění kybernetického bezpečnostního incidentu oznámení, v němž aktualizuje informace uvedené v odstavci 1, předloží prvotní posouzení kybernetického bezpečnostního incidentu a uvede dopad a indikátory kompromitace, pokud jsou k dispozici; poskytovatel regulovaných služeb vytvářejících důvěru podle přímo použitelného předpisu Evropské unie předloží toto oznámení do 24 hodin po zjištění kybernetického bezpečnostního incidentu,

...

c) nejpozději do 30 dnů ode dne předložení oznámení podle písmene a) závěrečnou zprávu o vyřešení kybernetického bezpečnostního incidentu; v případě, že po uplynutí uvedené lhůty kybernetický bezpečnostní incident stále trvá, předloží poskytovatel regulované služby bez zbytečného odkladu po uplynutí lhůty průběžnou zprávu o aktuálním stavu zvládání kybernetického bezpečnostního incidentu, a poté nejpozději do 30 dnů ode dne, kdy došlo k vyřešení kybernetického bezpečnostního incidentu závěrečnou zprávu o vyřešení kybernetického bezpečnostního incidentu.

**Překlad do Microsoft 365 a Azure**

- Jen když Úřad podle odstavce 2 sdělí významný dopad na kybernetický prostor státu
- Úkoly v incidentu s lhůtou 72 hodin od zjištění a 30 dní od oznámení
- Dotčená aktiva, indikátory kompromitace a časová osa z incidentu v Sentinelu

| Zjištěno | Stav | Mezera |
|---|---|---|
| Postup ani podklady pro oznámení a závěrečnou zprávu neexistují. Bez rozhodnutí o hlášení nejde lhůty ani spustit. | **Mezera** | M-07 |

## 4.8 Bezpečnost komunikačních sítí — § 18

### § 18 písm. b), d) a e) — řízení komunikace a vzdálené správy

> **§ 18 písm. b), d) a e) vyhlášky č. 409/2025 Sb.**
>
> Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to včetně jejího síťového perimetru
> ...
> b) zajistí řízení komunikace v rámci komunikační sítě,
> ...
> d) zajistí řízení vzdálené správy technických aktiv,
> e) povoluje v souladu s písmeny b) až d) pouze takovou komunikaci, která je nezbytná pro řádné zajištění regulované služby,

**Překlad do Microsoft 365 a Azure**

- Skupiny zabezpečení sítě s povoleným jen nutným provozem mezi vrstvami portálu
- Databáze, úložiště a Key Vault jen přes privátní koncové body
- Servery bez veřejné adresy, vzdálená správa jen přes Azure Bastion

| Zjištěno | Stav | Mezera |
|---|---|---|
| Podsítě portálu propouštějí jen povolený provoz, databáze, úložiště ani Key Vault nejsou dostupné z internetu. Servery se spravují jen přes Azure Bastion. | Splněno | — |

## 4.9 Správa a ověřování identit — § 19

### § 19 odst. 2 písm. a) — vícefaktorová autentizace

> **§ 19 odst. 2 písm. a) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba při ověření identity administrátorů, uživatelů a technických aktiv
> a) využívá autentizační mechanismus, který je založen na vícefaktorové autentizaci s alespoň dvěma různými typy faktorů, nebo využívá autentizační mechanismus, který je založen na aktuálně odolné kontinuální autentizaci založené na modelu nulové důvěry, a

**Překlad do Microsoft 365 a Azure**

- Conditional Access s vícefaktorovou autentizací pro všechny uživatele a aplikace
- Výjimka jen pro dva nouzové účty, které se přihlašují klíčem FIDO2

| Zjištěno | Stav | Mezera |
|---|---|---|
| Vícefaktorová autentizace platí pro všechny účty kromě 4 sdílených účtů dispečinku, které politika vylučuje a které se přihlašují jen heslem. | Částečně | M-08 |

### § 19 odst. 3 — evidence účtů bez vícefaktorové autentizace

> **§ 19 odst. 3 vyhlášky č. 409/2025 Sb.**
>
> (3) Povinná osoba do doby splnění požadavků podle odstavce 2 písm. a) vede evidenci technických aktiv, účtů a autentizačních mechanismů, které tyto požadavky nesplňují, a to včetně odůvodnění.

**Překlad do Microsoft 365 a Azure**

- Účty vyloučené z vícefaktorové autentizace v jedné skupině jako podklad evidence
- Odůvodnění a termín nápravy u každého účtu vede organizace

| Zjištěno | Stav | Mezera |
|---|---|---|
| Evidence neexistuje. Čtyři sdílené účty jsou z politiky vyloučené bez odůvodnění. | **Mezera** | M-08 |

## 4.10 Řízení přístupových práv a oprávnění — § 20

### § 20 písm. a) až c) — centrální nástroj pro práva a oprávnění

> **§ 20 písm. a) až c) vyhlášky č. 409/2025 Sb.**
>
> Povinná osoba pro řízení přístupových práv a oprávnění využívá nástroj,
> a) který je centralizovaný s ohledem na vazby mezi aktivy,
> b) kterým řídí práva pro přístup k jednotlivým aktivům a
> c) kterým řídí oprávnění pro čtení a zápis informací a dat a změnu oprávnění.

**Překlad do Microsoft 365 a Azure**

- Entra ID jako jediný zdroj identit a skupin pro Microsoft 365, Azure a portál
- Role Azure RBAC pro přístup k prostředkům i ke čtení a zápisu dat

| Zjištěno | Stav | Mezera |
|---|---|---|
| Přístup k Microsoft 365, Azure i správě portálu řídí centrálně Entra ID a role Azure, k datům portálu se přistupuje přes role Azure RBAC. | **Splněno** | — |

## 4.11 Detekce událostí — § 21

### § 21 odst. 2 písm. a) až c) a f) — ochrana a detekce na technických aktivech

> **§ 21 odst. 2 písm. a) až c) a f) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba používá s ohledem na vazby mezi aktivy pro detekci kybernetických bezpečnostních událostí centrálně spravovaný nástroj, který u jednotlivých relevantních technických aktiv zajišťuje
> a) nepřetržitou a automatickou ochranu před škodlivým kódem,
> b) řízení a sledování používání vyměnitelných zařízení a datových nosičů,
> c) řízení automatického spouštění obsahu, zejména u vyměnitelných zařízení a datových nosičů,
> ...
> f) detekci kybernetických bezpečnostních událostí technických aktiv a

**Překlad do Microsoft 365 a Azure**

- Defender for Endpoint Plan 1 s řízením vyměnitelných zařízení na zařízeních v Intune
- Automatické spouštění vypnuté nastavením v Intune
- Plány Defender for Cloud pro App Service, Azure SQL, úložiště a Key Vault

| Zjištěno | Stav | Mezera |
|---|---|---|
| Zařízení v Intune a servery integrace mají ochranu v reálném čase, vyměnitelná média a automatické spouštění jsou řízené. App Service, databáze, úložiště a Key Vault portálu plán Defender for Cloud nemají. | Částečně | M-09 |

## 4.12 Zaznamenávání událostí — § 22

### § 22 odst. 2 písm. d) — záznamy určených technických aktiv

> **§ 22 odst. 2 písm. d) vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba zaznamenává bezpečnostní a relevantní provozní události
> ...
> d) technických aktiv určených podle odstavce 1 písm. a).

**Překlad do Microsoft 365 a Azure**

- Diagnostická nastavení prostředků portálu do Sentinelu, vynucená Azure Policy
- Auditování Azure SQL Database

| Zjištěno | Stav | Mezera |
|---|---|---|
| Servery integrace posílají záznamy do Sentinelu. App Service, Application Gateway, databáze, úložiště ani Key Vault diagnostická nastavení nemají. | Částečně | M-09 |

### § 22 odst. 5 písm. c) — uchování záznamů 18 měsíců

> **§ 22 odst. 5 písm. c) vyhlášky č. 409/2025 Sb.**
>
> (5) Povinná osoba dále s ohledem na události zaznamenané podle odstavce 2
> ...
> c) uchovává záznamy těchto událostí alespoň po dobu 18 měsíců.

**Překlad do Microsoft 365 a Azure**

- Celková retence bezpečnostních tabulek 550 dní, 18 měsíců je zhruba 548 dní
- Po 90 dnech přechod do levnějšího dlouhodobého uchování
- Auditní log mimo Exchange, SharePoint a Teams kopírovat do Sentinelu

| Zjištěno | Stav | Mezera |
|---|---|---|
| Tabulky v Sentinelu mají retenci 90 dní, auditní log Microsoft 365 (Audit Standard) 180 dní, přihlašovací a auditní záznamy Entra ID s P1 30 dní. | Mezera | M-10 |

## 4.13 Vyhodnocování událostí — § 23

### § 23 odst. 1 písm. a) až c) — vyhodnocování událostí a včasné varování

> **§ 23 odst. 1 písm. a) až c) vyhlášky č. 409/2025 Sb.**
>
> (1) Povinná osoba používá nástroj pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí detekovaných podle § 21, který zajišťuje
> a) sběr, vyhledávání a seskupování souvisejících záznamů za účelem detekce kybernetických bezpečnostních událostí,
> b) nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech, včasné varování vybraných bezpečnostních rolí a dalších relevantních osob a
> c) vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů.

**Překlad do Microsoft 365 a Azure**

- Microsoft Sentinel s analytickými pravidly a seskupováním výstrah do incidentů
- Upozornění do Teams a na telefon pohotovosti podle závažnosti incidentu
- Eskalace na další roli, když incident do 2 hodin nikdo nepřevezme

| Zjištěno | Stav | Mezera |
|---|---|---|
| Sentinel vyhodnocuje záznamy nepřetržitě 38 aktivními pravidly. Upozornění ale chodí jen e-mailem do schránky IT, kterou mimo pracovní dobu nikdo nečte. | Částečně | M-07 |

## 4.14 Aplikační bezpečnost — § 24

### § 24 odst. 3 písm. a) — ochrana před neoprávněnou činností

> **§ 24 odst. 3 písm. a) vyhlášky č. 409/2025 Sb.**
>
> (3) Povinná osoba v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací, transakcí a přenášených identifikátorů relací před
> a) neoprávněnou činností a

**Překlad do Microsoft 365 a Azure**

- Portál jen přes HTTPS s TLS 1.2 a vyšším, identifikátory relací jen šifrovaně
- Application Gateway s WAF v režimu prevence, sada pravidel OWASP

| Zjištěno | Stav | Mezera |
|---|---|---|
| Portál přijímá jen HTTPS s TLS 1.2 a vyšším a WAF je v režimu prevence. Ochranu relací v kódu aplikace analýza neposuzovala. | Splněno | — |

### § 24 odst. 3 písm. b) — ochrana před popřením provedených činností

> **§ 24 odst. 3 písm. b) vyhlášky č. 409/2025 Sb.**
>
> (3) Povinná osoba v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací, transakcí a přenášených identifikátorů relací před
> ...
> b) popřením provedených činností.

**Překlad do Microsoft 365 a Azure**

- Auditování Azure SQL a diagnostické záznamy App Service v Sentinelu
- Záznam činností uživatelů v portálu s identitou a časem, požadavek na dodavatele

| Zjištěno | Stav | Mezera |
|---|---|---|
| Portál ani databáze činnosti uživatelů nezaznamenávají, zpětně nejde doložit, kdo transakci provedl. | Mezera | M-09 |

## 4.15 Kryptografické algoritmy — § 25

### § 25 odst. 1 písm. a) — aktuálně odolné algoritmy

> **§ 25 odst. 1 písm. a) vyhlášky č. 409/2025 Sb.**
>
> (1) Povinná osoba při zajištění bezpečnosti technických aktiv a jejich komunikace
> a) používá pouze aktuálně odolné kryptografické algoritmy,

**Překlad do Microsoft 365 a Azure**

- Minimální verze TLS 1.2 na všech prostředcích portálu
- Politika TLS na Application Gateway bez zastaralých sad šifer
- Šifrování dat v klidu AES-256 v úložišti a Azure SQL

| Zjištěno | Stav | Mezera |
|---|---|---|
| Všechny prostředky portálu vyžadují TLS 1.2 a vyšší, data v klidu jsou šifrovaná AES-256. | Splněno | — |

### § 25 odst. 3 písm. b) — nástroj pro správu klíčů a certifikátů

> **§ 25 odst. 3 písm. b) vyhlášky č. 409/2025 Sb.**
>
> (3) Povinná osoba v případě využívání kryptografických klíčů a certifikátů pro ochranu technických aktiv a komunikační sítě používá
> ...
> b) nástroj pro správu kryptografických klíčů a certifikátů, který
> 1. zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů,
> 2. umožní kontrolu a audit a
> 3. zajistí důvěrnost a integritu kryptografických klíčů.

**Překlad do Microsoft 365 a Azure**

- Azure Key Vault pro certifikát a tajné klíče portálu, přístup přes Azure RBAC
- Ochrana proti vymazání a auditní záznamy Key Vault v Sentinelu

| Zjištěno | Stav | Mezera |
|---|---|---|
| Certifikát i tajné klíče jsou v Key Vault s ochranou proti vymazání. Auditní záznamy Key Vault se nesbírají, kontrolu a audit nejde doložit. | Částečně | M-09 |

# 4.16 Dostupnost regulované služby — § 26

## § 26 odst. 2 — pravidelné zálohy

> **§ 26 odst. 2 vyhlášky č. 409/2025 Sb.**
>
> (2) Povinná osoba pro zajišťování dostupnosti regulované služby v souladu s odstavcem 1 vytváří pravidelné zálohy konfigurací a nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby v případě kybernetického bezpečnostního incidentu.

**Překlad do Microsoft 365 a Azure**

- Azure Backup pro servery a dlouhodobé zálohy databáze portálu
- Záloha dat Microsoft 365 přes Microsoft 365 Backup nebo nástroj třetí strany
- Microsoft data za retenčními lhůtami nezálohuje, záloha je na organizaci

| Zjištěno | Stav | Mezera |
|---|---|---|
| Servery se zálohují denně. Databáze portálu má jen automatické zálohy na 7 dní a data Microsoft 365 se nezálohují. | Částečně | M-11, M-12 |

## § 26 odst. 3 písm. a) a b) — test obnovy a jeho dokumentace

> **§ 26 odst. 3 písm. a) a b) vyhlášky č. 409/2025 Sb.**
>
> (3) Povinná osoba u záloh vytvářených podle odstavce 2 zajistí
> a) pravidelné testování jejich integrity, dostupnosti a obnovitelnosti,
> b) dokumentování výsledků testů provedených podle odstavce 3 písm. a),

**Překlad do Microsoft 365 a Azure**

- Čtvrtletní zkušební obnova databáze a serveru do izolovaného prostředí
- Protokol o testu s dobou obnovy porovnanou s cíli podle § 15

| Zjištěno | Stav | Mezera |
|---|---|---|
| Obnova ze záloh se nikdy nezkoušela a protokol o testu neexistuje. | Mezera | M-12 |

# 5. Mezery

Dvě nejzávažnější mezery v plném znění. Všech 12 je v registru mezer v příloze.

## 5.1 M-08 — Sdílené účty dispečinku se přihlašují jen heslem

| Vlastnost | Hodnota |
|---|---|
| Ustanovení | § 13 odst. 2 písm. b), § 19 odst. 2 písm. a), § 19 odst. 3 |
| Priorita | **Kritická** |
| Pracnost | Střední |

### 5.1.1 Zjištěný stav

Politika Conditional Access s vícefaktorovou autentizací vylučuje skupinu čtyř sdílených účtů dispečinku, které se přihlašují jen heslem. Dva z nich se za 30 dní přihlásily i z adres mimo síť dispečinku. Evidenci účtů, které požadavek nesplňují, organizace nevede.

*Ověření: přihlášení sdílených účtů za 30 dní*

```
SigninLogs
| where TimeGenerated > ago(30d)
| where UserPrincipalName startswith "dispecink"
| summarize Prihlaseni = count(), Adresy = make_set(IPAddress)
    by UserPrincipalName, AuthenticationRequirement
```

### 5.1.2 Dopad

Kdo získá heslo, má odkudkoli přístup ke sdílené schránce hlášení poruch a k týmu pohotovosti. Činnost pod sdíleným účtem nejde přiřadit konkrétnímu dispečerovi.

### 5.1.3 Doporučení

- Dispečerům zřídit osobní účty a sdílenou schránku zpřístupnit delegací.
- Na sdílených stanicích dispečinku přihlašovat klíčem FIDO2 s PINem, který splní vícefaktorovou autentizaci i při střídání směn.
- Do přechodu omezit sdílené účty politikou Conditional Access na síť dispečinku a spravovaná zařízení a zapsat je do evidence podle § 19 odst. 3. Riziko to sníží, požadavek odstavce 2 to nesplní.

## 5.2 M-07 — Z incidentu nevede určená cesta k hlášení

| Vlastnost | Hodnota |
|---|---|
| Ustanovení | § 14 odst. 1 písm. c) a g), § 23 odst. 1 písm. a) až c); zákon § 15 odst. 1, § 16 odst. 1, § 16 odst. 3 písm. a) a c) |
| Priorita | **Vysoká** |
| Pracnost | Střední |

### 5.2.1 Zjištěný stav

Za 90 dní vzniklo v Sentinelu 212 incidentů, 64 % z nich bez řešitele, u závažných trvá první zásah v mediánu 31 hodin. Upozornění chodí jen e-mailem do schránky IT. Z incidentu nejde poznat, zda se projevil ve stanoveném rozsahu, ani kdo posoudil, zda podléhá hlášení.

*Ověření: řešitelé a doba do prvního zásahu za 90 dní*

```
SecurityIncident
| where CreatedTime > ago(90d)
| summarize arg_max(LastModifiedTime, *) by IncidentNumber
| summarize Incidenty = count(),
    BezResitele = countif(isempty(tostring(Owner.assignedTo))),
    MedianHodin = percentile(
        datetime_diff("hour", FirstModifiedTime, CreatedTime), 50)
    by Severity
```

### 5.2.2 Dopad

Hlásí se každý incident ve stanoveném rozsahu s původem v kybernetickém prostoru, u kterého nelze vyloučit úmyslné zavinění, bez ohledu na významnost dopadu. Prvotní hlášení je nutné do 24 hodin po zjištění, dnes trvá první zásah 31 hodin.

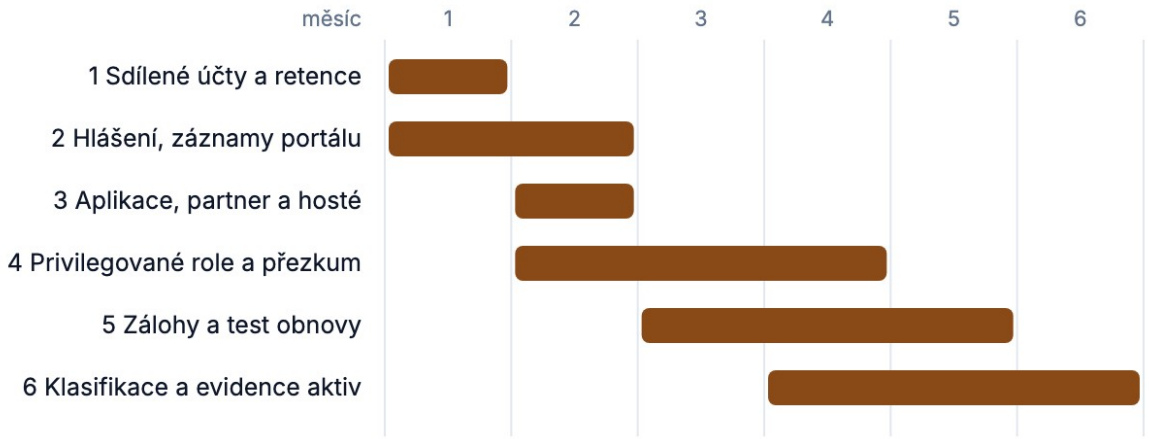
### 5.2.3 Doporučení

- Kdo incidenty přebírá, posuzuje a hlásí přes Portál Úřadu, určí organizace.
- Watchlist aktiv v rozsahu a automatizace, která incidentu přidá úkol posoudit hlášení.
- Upozornění do Teams a na telefon pohotovosti, lhůtu 24 hodin hlídat v Sentinelu.
- Rozhodnutí o hlášení zapsat do incidentu, doklad vznikne dotazem nad SecurityIncident.

# 6. Roadmapa

Pořadí je podle priority a závislostí. Krok 1 řeší jedinou kritickou mezeru a retenci, u které každý den odkladu znamená nevratně ztracené záznamy. Dočasné role a přezkum přístupu čekají na licence Entra ID P2, náhradní čtvrtletní přezkum exportem jde spustit hned.

*Harmonogram (měsíce)*




*Pracnost kroku je nejvyšší pracnost z jeho mezer*

| Krok | Obsah | Mezery | Pracnost |
|---|---|---|---|
| 1 | Osobní účty dispečerů s klíči FIDO2, retence záznamů 550 dní | M-08, M-10 | Střední |
| 2 | Cesta od incidentu k hlášení do 24 hodin, záznamy a detekce portálu | M-07, M-09 | Střední |
| 3 | Omezit aplikace s přístupem k poště, zúžit přístup partnera, odebrat neaktivní hosty | M-03, M-04 | Střední |
| 4 | Licence Entra ID P2, dočasné role, oddělené účty správců, přezkum přístupu | M-05, M-06 | Střední |
| 5 | Zálohy Microsoft 365 a databáze portálu, test obnovy s protokolem | M-11, M-12 | Střední |
| 6 | Pravidla klasifikace a popisky citlivosti, tagy a evidence prostředků portálu | M-01, M-02 | Vysoká |

# 7. Přílohy

## 7.1 Registr mezer

*§ bez dalšího označení je vyhláška č. 409/2025 Sb., zákon je zákon č. 264/2025 Sb.*

| ID | Mezera | Ustanovení | Priorita | Pracnost |
|---|---|---|---|---|
| M-01 | Pravidla klasifikace a označování chybějí, Microsoft 365 nemá popisky citlivosti | § 7 písm. h) body 3 a 4 | Střední | Vysoká |
| M-02 | Prostředky portálu nejsou v evidenci aktiv ani označené | § 7 písm. f); zákon § 12 odst. 3 | Nízká | Nízká |
| M-03 | Aplikace třetích stran mají přístup ke všem schránkám | § 9 odst. 1 písm. c), § 13 odst. 2 písm. c) | Vysoká | Střední |
| M-04 | Partner má roli globálního správce, hosté dodavatele se neodebírají | § 9 odst. 1 písm. c), § 13 odst. 2 písm. j) | Střední | Nízká |
| M-05 | Privilegované role jsou trvalé a široké, správci nemají oddělený účet | § 13 odst. 2 písm. b) | Vysoká | Střední |
| M-06 | Přístupová práva se nepřezkoumávají ani neupravují při změně pozice | § 13 odst. 2 písm. h), § 13 odst. 2 písm. i) | Vysoká | Střední |
| M-07 | Z incidentu nevede určená cesta k hlášení | § 14 odst. 1 písm. c) a g), § 23 odst. 1 písm. a) až c); zákon § 15 odst. 1, § 16 odst. 1, § 16 odst. 3 písm. a) a c) | Vysoká | Střední |
| M-08 | Sdílené účty dispečinku se přihlašují jen heslem | § 13 odst. 2 písm. b), § 19 odst. 2 písm. a), § 19 odst. 3 | Kritická | Střední |
| M-09 | Portál není zdrojem záznamů ani detekce | § 21 odst. 2 písm. a) až c) a f), § 22 odst. 2 písm. d), § 24 odst. 3 písm. b), § 25 odst. 3 písm. b) | Vysoká | Střední |
| M-10 | Záznamy se uchovávají kratší dobu než 18 měsíců | § 22 odst. 5 písm. c) | Vysoká | Nízká |
| M-11 | Data Microsoft 365 se nezálohují | § 26 odst. 2 | Střední | Střední |
| M-12 | Databázi portálu jde obnovit jen 7 dní zpět, obnova se nezkouší | § 26 odst. 2, § 26 odst. 3 písm. a) a b) | Střední | Nízká |

## 7.2 Důkazní balík

*Doklady s datem a zdrojem, opakovatelné; k chybějícím nastavením vzniknou po odstranění mezery*

| Doklad | Odkud se exportuje | Ustanovení |
|---|---|---|
| Prostředky portálu s tagy | Azure Resource Graph | zákon § 12 odst. 3, § 7 písm. f) |
| Přístupy partnera, aplikací a hostů | Entra ID, Microsoft Graph | § 9 odst. 1 písm. c), § 13 odst. 2 písm. j) |
| Oprávnění aplikací k poště | Entra ID, Exchange Online | § 13 odst. 2 písm. c) |
| Historie nasazení portálu | Azure DevOps | § 11 odst. 2 písm. a) |
| Politiky Conditional Access | Entra ID, Microsoft Graph | § 12 odst. 2 písm. a), § 19 odst. 2 písm. a) |
| Účty bez vícefaktorové autentizace | Entra ID, skupina výjimek | § 19 odst. 3 |
| Role, jejich přiřazení a přezkumy | Entra ID, PIM, Azure RBAC | § 13 odst. 2 písm. b), h), § 20 |
| Incidenty a rozhodnutí o hlášení | Sentinel, SecurityIncident | § 14 odst. 1 písm. c), g), zákon § 15, § 16 |
| Pravidla Sentinelu a plány Defenderu | Sentinel, Defender for Cloud | § 21 odst. 2, § 23 odst. 1 |
| Diagnostika a retence tabulek | Azure Policy, Log Analytics | § 22 odst. 2 písm. d), odst. 5 písm. c) |
| Síť, TLS a WAF portálu | Azure Resource Graph | § 18, § 24 odst. 3 písm. a), § 25 odst. 1 |
| Záznamy činností v portálu | App Service, Azure SQL | § 24 odst. 3 písm. b) |
| Key Vault a jeho auditní záznamy | Azure Resource Graph | § 25 odst. 3 písm. b) |
| Zálohy a protokol testu obnovy | Azure Backup, Azure SQL | § 26 odst. 2, odst. 3 písm. a), b) |
| Auditní zprávy Microsoftu | Service Trust Portal | § 9 odst. 2 písm. c) |

## 7.3 Povinnosti mimo rozsah

Nejde o mezery analýzy. Organizace je zajišťuje a dokládá mimo Microsoft 365 a Azure.

- Opatření bez odrazu v cloudu: § 3, § 4, § 5, § 6, § 8, § 10, § 15, § 16, § 17, § 27.
- Stanovený rozsah podle zákona § 12 odst. 2 a 5, pravidla pro dodavatele a významní dodavatelé podle § 9 odst. 1 písm. a), b), d) až g) a § 9 odst. 2.
- Určení významných změn podle § 11 odst. 1, procesy zvládání incidentů podle § 14 odst. 1 písm. a) a b).
- Skenování zranitelností a penetrační testy (§ 24 odst. 4 až 6), systémy mimo cloud.