BEARCLAVE

Report z analýzy

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

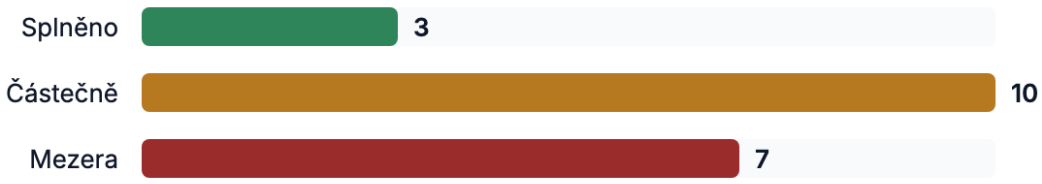
Organizace je poskytovatelem regulované služby v režimu nižších povinností: průmyslová výroba potravin je služba 8.1 přílohy vyhlášky č. 408/2025 Sb., u které příloha střednímu podniku, a tedy i organizaci se zhruba 150 zaměstnanci, určuje právě režim nižších povinností. Oproti vyšším povinnostem to znamená užší vyhlášku č. 410/2025 Sb. místo 409/2025 Sb. a hlášení jen incidentů s významným dopadem, a to Národnímu CERT, ne Úřadu.

Nižší	**20**	**3**	**10**
režim povinností podle přílohy vyhlášky 408/2025, služba 8.1	ustanovení vyhlášky a zákona se odráží v Microsoft 365 a Azure	z nich splněno	mezer, z toho 1 kritická

Stav 20 ustanovení: splněno 3, částečně 10, mezera 7. V pořádku je správa zařízení, zaznamenávání událostí a šifrování.

Kritická je jediná mezera: na ERP server se lze přes RDP připojit z celého internetu a vestavěný účet správce chrání jen heslo. Doporučujeme začít jí a hned potom stanovit, jak se posuzuje významnost incidentu a kdo ho hlásí Národnímu CERT. Bez toho organizace nepozná, co má hlásit.

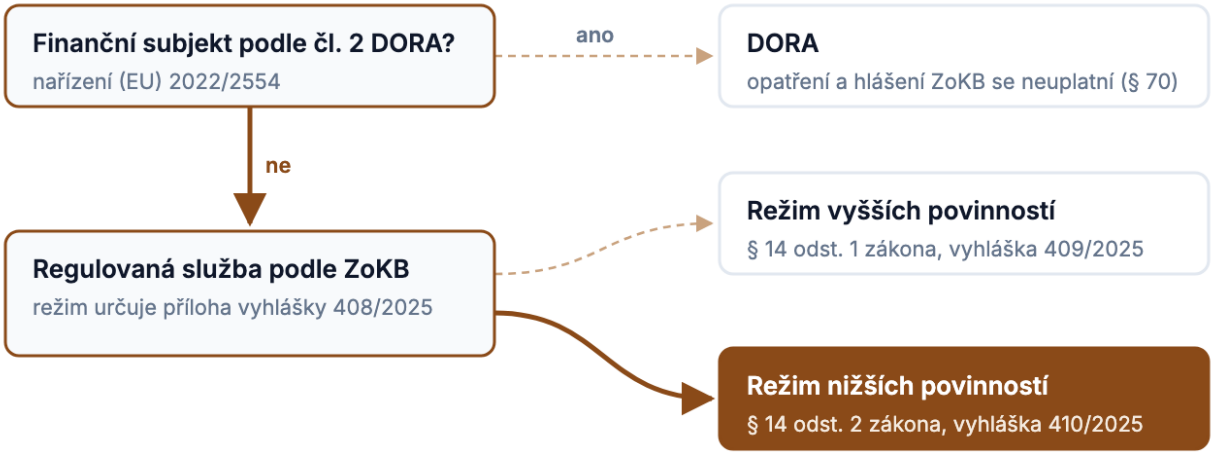
Stav 20 namapovaných ustanovení



2. Režim a rozsah

2.1 Určení režimu

Režim vyplývá z rozhodnutí o registraci regulované služby a z vyhodnocení organizace. Analýza ho přebírá.



příloha, bod 8.1 vyhlášky č. 408/2025 Sb.

Potravinářský podnik podle přímo použitelného předpisu Evropské unie, který se zabývá průmyslovou výrobou potravin, je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým podnikem, nebo středním podnikem.

§ 8 odst. 1 až 3 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.
(3) Je-li regulovaná služba registrována rozhodnutím Úřadu na základě splnění podmínek pro registraci podle § 5, je její poskytovatel v režimu vyšších povinností.

Regulovaná služba	Podmínka	Režim	Měří se proti	Hlášení
8.1 Průmyslová výroba potravin	potravinářský podnik, střední podnik; služba není registrovaná podle § 5 zákona	Nižší povinnosti	zákon § 14 odst. 2, vyhláška 410/2025	§ 15 odst. 2 a § 16 zákona, Národní CERT

Co režim nižších povinností mění proti vyšším

Oblast	Nižší povinnosti — organizace	Vyšší povinnosti
Opatření	13 opatření, vyhláška 410/2025	25 opatření, vyhláška 409/2025
Co se hlásí, § 15	jen incidenty s významným dopadem	i incidenty bez významného dopadu
Komu, § 15 a 16	Národní CERT	Úřad
Začátek plnění	rok od doručení rozhodnutí o registraci	stejně, § 13 odst. 4 a § 15 odst. 4

2.2 Prostředí

Prostředí	Hodnota
Organizace	průmyslová výroba potravin, střední podnik, zhruba 150 zaměstnanců
Microsoft 365	Business Premium pro 140 uživatelů: Entra ID P1, Intune, Defender for Business, Defender for Office 365 Plan 1; identity jen v cloudu
Zařízení	stanice s Windows 11 a telefony v Intune, osobní telefony s ochranou aplikací
Azure	dva servery ERP, VPN do závodu, Azure Backup, Log Analytics, Defender for Cloud zdarma
Správa	dva interní správci IT, externí správce IT se dvěma účty hostů
Dohled	incidenty v portálu Microsoft Defender, bez Sentinelu a dohledového centra

Stanovený rozsah podle § 12 zákona, jak ho předala organizace

Aktivum	Kde běží	Co z něj analýza pokrývá
Plánování výroby, receptury	ERP v Azure	servery, síť, zálohy a přístup, ne účty uvnitř ERP
Dokumentace výroby a kvality	SharePoint	přístup, sdílení a zálohy
Objednávky a expedice	ERP, pošta, Teams	účty, pošta, sdílený účet expedice
Identita a zařízení	Microsoft 365	účty, role, ověřování, hosté, zařízení v Intune
Výrobní linky a jejich řízení	síť závodu	nepokrývá

2.3 Co analýza není

- Není právní posouzení. Režim a stanovený rozsah přebírá od organizace.
- Nepokrývá výrobní linky a jejich řídicí systémy, síť závodu ani účty uvnitř aplikace ERP.
- Nenahrazuje přehled bezpečnostních opatření (§ 3 odst. 2), je jeho podkladem.

3. Relevantní ustanovení

Zákon stanoví pro nižší povinnosti 13 opatření, obsah jim dává vyhláška č. 410/2025 Sb. Mapuje se 8 opatření s odrazem v Microsoft 365 a Azure, zbylých 5 je v příloze Povinnosti mimo rozsah.

> **§ 3 odst. 1 vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba při zajišťování kybernetické bezpečnosti
> a) zavede a provádí bezpečnostní opatření, která jsou přiměřená bezpečnostním potřebám, a
> b) zavede a provádí alespoň bezpečnostní opatření podle odstavců 2 až 6, § 4 až 6 a § 10.

Opatření podle § 14 odst. 2 zákona a jejich místo ve vyhlášce 410/2025

Písm.	Opatření	Vyhláška	Závaznost	Odraz v M365 a Azure
a)	systém zajišťování minimální kybernetické bezpečnosti	§ 3 odst. 1 až 3, 5 a 6	Vždy	Žádný
b)	požadavky na vrcholné vedení	§ 4	Vždy	Žádný
c)	řízení aktiv	§ 3 odst. 4	Vždy	Žádný
d)	řízení rizik	samostatně neupraveno	—	Žádný
e)	bezpečnost lidských zdrojů	§ 5	Vždy	Žádný
f)	řízení kontinuity činností	§ 6	Vždy	Částečný
g)	řízení přístupu	§ 7	Podle potřeb	Přímý
h)	řízení identit a jejich oprávnění	§ 8	Podle potřeb	Přímý
i)	detekce a zaznamenávání kybernetických bezpečnostních událostí	§ 9	Podle potřeb	Přímý
j)	řešení kybernetických bezpečnostních incidentů	§ 10 a 14	Vždy	Částečný
k)	bezpečnost komunikačních sítí	§ 11	Podle potřeb	Přímý
l)	aplikační bezpečnost	§ 12	Podle potřeb	Přímý
m)	kryptografické algoritmy	§ 13	Podle potřeb	Přímý

Vždy: § 3 odst. 1 písm. b). Podle potřeb: nezavedení odůvodní organizace v přehledu bezpečnostních opatření (§ 3 odst. 2 písm. a) bod 3). Organizace nic takového neodůvodňuje, analýza proto měří plné znění. Řízení rizik vyhláška samostatně neupravuje, promítá se do § 3 odst. 1 písm. a) a odst. 5.

4. Mapování

Každé ustanovení má doslovné znění, překlad do nastavení Microsoft 365 a Azure a zjištěný stav. Splněno: nastavení platí v celém stanoveném rozsahu, částečně: s výjimkami, mezera: nastavení chybí.

Přehled 20 ustanovení

Ustanovení	Oblast	Stav	Mezera
§ 6 písm. c)	zálohy	Částečně	M-04
§ 7 odst. 1 písm. a) a b)	přístupová práva a jedinečné účty	Částečně	M-01, M-02, M-05
§ 7 odst. 1 písm. c)	mobilní a nespravovaná zařízení	Splněno	—
§ 7 odst. 1 písm. d)	přezkum přístupových práv	Mezera	M-03
§ 7 odst. 1 písm. e) a f)	změny a odchody	Částečně	M-03
§ 8 odst. 1	nástroj pro řízení identit	Částečně	M-05
§ 8 odst. 2	vícefaktorová autentizace	Částečně	M-01, M-05
§ 8 odst. 3 a 4	klíče, certifikáty a pravidla hesel	Mezera	M-01, M-05
§ 8 odst. 5	výchozí údaje, obnova a nouzové účty	Částečně	M-05
§ 9 odst. 1	detekce událostí	Částečně	M-05, M-06, M-08
§ 9 odst. 2	zaznamenávání událostí	Splněno	—
§ 9 odst. 3	doba uchování záznamů	Mezera	M-07
§ 10 písm. b), d) až f)	posuzování a hlášení incidentů	Mezera	M-08
§ 14 odst. 1 a 2	významnost dopadu incidentu	Mezera	M-08
zákon § 15 odst. 2 a 3	hlášení Národnímu CERT podle zákona	Mezera	M-08
zákon § 16 odst. 1, 3 a 4	lhůty a způsob hlášení podle zákona	Mezera	M-08
§ 11	bezpečnost komunikační sítě	Částečně	M-05
§ 12	aplikační bezpečnost	Částečně	M-06, M-10
§ 13 odst. 1	kryptografické algoritmy	Splněno	—
§ 13 odst. 2 písm. a)	bezpečná komunikace a e-mail	Částečně	M-09

4.1 § 6 — řízení kontinuity činností

§ 6 písm. c) — zálohy

> **§ 6 písm. c) vyhlášky č. 410/2025 Sb.**
>
> Povinná osoba v rámci řízení kontinuity činností
>
> ...
>
> c) vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

Překlad do Microsoft 365 a Azure

- ERP servery: Azure Backup s neměnným trezorem. Microsoft 365: Microsoft 365 Backup nebo záloha třetí strany, konfigurace Entra ID a Intune exportem přes Microsoft Graph.

Zjištěno	Stav	Mezera
ERP servery se zálohují denně s uchováním 30 dní. Microsoft 365, včetně výrobní dokumentace v SharePointu, ani konfigurace tenantu se nezálohují a po uplynutí lhůt koše Microsoft data neobnoví.	Částečně	M-04

4.2 § 7 — řízení přístupu

§ 7 odst. 1 písm. a) a b) — přístupová práva a jedinečné účty

> **§ 7 odst. 1 písm. a) a b) vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba řídí přístup k aktivům a v rámci něj
> a) přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu jejich práce a jedinečný identifikátor daného typu účtu, přičemž od sebe odděluje uživatelské a administrátorské účty jedné osoby,
> b) řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv,

Překlad do Microsoft 365 a Azure

- Vlastní účet pro každého, správcům oddělený administrátorský účet s nejužší rolí, servisní účty nahradit identitami aplikací s vlastníkem. Dočasné role v PIM vyžadují Entra ID P2.

Zjištěno	Stav	Mezera
Interní správci pracují s běžnými účty s trvalou rolí globálního správce, stejně jako oba hosté externího správce. Účet expedice sdílí šest lidí, na ERP servery se správci hlásí jedním vestavěným účtem a tři servisní účty nemají vlastníka.	Částečně	M-01, M-02, M-05

§ 7 odst. 1 písm. c) — mobilní a nespravovaná zařízení

> **§ 7 odst. 1 písm. c) vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba řídí přístup k aktivům a v rámci něj
>
> …
>
> c) zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných obdobných technických aktiv, popřípadě i bezpečnostní opatření spojená s využitím technických aktiv, která povinná osoba nemá ve své správě,

Překlad do Microsoft 365 a Azure

- Firemní zařízení v Intune s pravidly shody, osobní telefony jen přes aplikace s ochranou Intune. Conditional Access pustí k datům jen vyhovující zařízení nebo chráněné aplikace.

Zjištěno	Stav	Mezera
Notebooky a firemní telefony jsou v Intune s pravidly shody, osobní telefony mají přístup jen přes chráněné aplikace. Jiný přístup Conditional Access blokuje.	Splněno	—

§ 7 odst. 1 písm. d) — přezkum přístupových práv

> **§ 7 odst. 1 písm. d) vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba řídí přístup k aktivům a v rámci něj
>
> …
>
> d) provádí pravidelné přezkoumání nastavení veškerých přístupových práv a oprávnění,

Překlad do Microsoft 365 a Azure

- Přezkum přístupu v Entra ID vyžaduje Entra ID P2 nebo Entra ID Governance. S licencí P1 čtvrtletní export rolí, skupin a hostů přes Microsoft Graph se schválením vlastníka.

Zjištěno	Stav	Mezera
Přístupová práva nikdo pravidelně nepřezkoumává.	Mezera	M-03

§ 7 odst. 1 písm. e) a f) — změny a odchody

> **§ 7 odst. 1 písm. e) a f) vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba řídí přístup k aktivům a v rámci něj
>
> ...
>
> e) zajistí bezodkladné odebrání nebo změnu přístupových práv a oprávnění při změně pozice nebo zařazení uživatelů nebo administrátorů a
> f) zajistí deaktivaci účtu a bezodkladné odebrání nebo změnu přístupových práv a oprávnění při ukončení nebo změně smluvního vztahu, na jehož základě došlo ke zřízení přístupu k aktivům.

Překlad do Microsoft 365 a Azure

- Při změně pozice nebo odchodu zablokovat účet, odvolat relace a odebrat skupiny a role podle kontrolního seznamu z personální agendy, hosty dodavatelů vázat na trvání smlouvy.

Zjištěno	Stav	Mezera
Účty blokuje IT ručně podle e-mailu z personálního. Aktivní zůstaly čtyři účty lidí, kteří odešli, a host bývalého dodavatele.	Částečně	M-03

4.3 § 8 — řízení identit a jejich oprávnění

Odstavce 3 a 4 platí jen do doby, než účet používá mechanismus podle předchozího odstavce. U účtů s vícefaktorovou autentizací se pravidla hesel neuplatní, u účtů jen s heslem ano.

Co z § 8 odst. 2 až 4 platí pro které účty

Účty	Ověření dnes	Co platí	Mezera
Uživatelé, správci a hosté	vícefaktorová autentizace	odst. 2 splněn, odst. 3 a 4 se neuplatní	—
Dva nouzové účty	klíč FIDO2	odst. 2 splněn	—
Tři servisní účty	jen heslo	bez odst. 2 i 3, platí pravidla hesel podle odst. 4	M-01
Sdílený účet expedice	jen heslo	platí pravidla hesel podle odst. 4	M-01
Místní účty ERP serverů	jen heslo	platí pravidla hesel podle odst. 4	M-05

§ 8 odst. 1 — nástroj pro řízení identit

> **§ 8 odst. 1 vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba pro řízení identit, přístupových práv a oprávnění používá nástroj, který zajišťuje
> a) řízení počtu možných neúspěšných pokusů o přihlášení,
> b) opětovné ověření identity po stanovené době nečinnosti,
> c) odolnost uložených a přenášených autentizačních údajů a
> d) řízení přístupových práv, oprávnění pro čtení a zápis informací a dat a změnu oprávnění.

Překlad do Microsoft 365 a Azure

- Entra ID: inteligentní uzamčení účtu, chráněné autentizační údaje, oprávnění přes skupiny a role Azure. Intune zamyká obrazovku, webové aplikace Microsoft 365 odhlašují nečinné relace.

Zjištěno	Stav	Mezera
Entra ID zamyká účet po 10 neúspěšných pokusech, Intune zamyká obrazovku po 10 minutách, web odhlašuje po 1 hodině nečinnosti. Místní účty ERP serverů ale stojí mimo Entra ID a spravují se ručně.	Částečně	M-05

§ 8 odst. 2 — vícefaktorová autentizace

> **§ 8 odst. 2 vyhlášky č. 410/2025 Sb.**
>
> (2) Povinná osoba pro ověření identity administrátorů, uživatelů a technických aktiv využívá autentizační mechanismus, který je založený 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.

Překlad do Microsoft 365 a Azure

- Conditional Access: vícefaktorová autentizace pro všechny uživatele, správce a hosty, správcům síla ověření odolná proti phishingu. Nouzové účty ji splní klíčem FIDO2.
- ERP servery: přihlášení účty Entra ID s vícefaktorovou autentizací z Conditional Access.

Zjištěno	Stav	Mezera
Conditional Access vyžaduje vícefaktorovou autentizaci u všech kromě tří servisních účtů a sdíleného účtu expedice, starší ověřování blokuje. Na ERP servery se správci přihlašují místním účtem jen heslem.	Částečně	M-01, M-05

§ 8 odst. 3 a 4 — klíče, certifikáty a pravidla hesel

§ 8 odst. 3 a 4 vyhlášky č. 410/2025 Sb.

(3) Povinná osoba do doby využívání autentizačního mechanismu podle odstavce 2 využívá autentizaci pomocí kryptografických klíčů nebo certifikátů.
(4) Povinná osoba do doby využívání autentizačního mechanismu podle odstavce 3 využívá nástroj založený na autentizaci pomocí identifikátoru účtu a hesla, kdy tento nástroj musí vynucovat pravidla
a) délky hesla alespoň
1. 12 znaků pro účty uživatelů,
2. 17 znaků pro účty administrátorů,
3. 22 znaků pro účty technických aktiv,
b) bezodkladné změny výchozího hesla pro ověření identity technických aktiv, přičemž nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,
c) neomezující použití malých a velkých písmen, číslic a speciálních znaků,
d) povinné změny hesla v intervalu alespoň jednou za 18 měsíců a
e) neumožňující uživatelům a administrátorům
1. zvolit si jednoduchá a často používaná hesla,
2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacích jmen, adres elektronické pošty, názvů systémů nebo obdobným způsobem a
3. opětovného použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.

Překlad do Microsoft 365 a Azure

- Servisní účty převést na identity aplikací ověřované certifikátem, tím pro ně platí odst. 3.
- Entra ID u cloudových účtů délku 12, 17 a 22 znaků ani paměť 12 hesel nevynutí. Účet jen s heslem v Entra ID proto odst. 4 nesplní a musí přejít na odst. 2 nebo 3.

Zjištěno	Stav	Mezera
Tři servisní účty, sdílený účet expedice a místní účty ERP serverů mají jen heslo. Pravidla odst. 4 nevynucuje Entra ID, které žádá 8 znaků a hesla nechává platit neomezeně, ani místní zásada serverů.	**Mezera**	M-01, M-05

§ 8 odst. 5 — výchozí údaje, obnova a nouzové účty

§ 8 odst. 5 vyhlášky č. 410/2025 Sb.

(5) Povinná osoba při řízení identit dále zajistí
a) důvěrnost při vytváření výchozích autentizačních údajů a při obnově přístupu,
b) změnu výchozího hesla nebo hesla sloužícího k obnově přístupu po jeho prvním použití,
c) zneplatnění hesla nebo identifikátoru sloužícího k obnově přístupu nejpozději do 24 hodin od jeho vytvoření,
d) bezodkladnou změnu přístupového hesla v případě důvodného podezření na jeho kompromitaci a
e) zabezpečení administrátorských účtů technických aktiv zejména určených pro případ obnovy po kybernetickém bezpečnostním incidentu a využívá tyto účty pouze v nezbytně nutných případech.

Překlad do Microsoft 365 a Azure

- Nástup a obnova dočasným přístupovým kódem (Temporary Access Pass) na jedno použití do 24 hodin, při podezření na kompromitaci reset hesla. Účty pro obnovu s klíčem nebo náhodným heslem v trezoru, jen pro nouzi.

Zjištěno	Stav	Mezera
Dočasný přístupový kód platí 8 hodin a jen jednou, nouzové účty mají klíče FIDO2 v trezoru. Vestavěný účet správce ERP serverů ale slouží k běžné správě.	Částečně	M-05

4.4 § 9 — detekce a zaznamenávání událostí

§ 9 odst. 1 — detekce událostí

> **§ 9 odst. 1 vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba při detekci kybernetických bezpečnostních událostí zajistí
> a) ověření a kontrolu přenášených dat na perimetru komunikační sítě, včetně blokování nežádoucí komunikace,
> b) použití nástroje pro nepřetržitou a automatickou ochranu před škodlivým kódem na technických aktivech, zejména na
> 1. serverech a
> 2. koncových stanicích,
> c) řízení automatického spouštění obsahu, zejména u vyměnitelných zařízení a datových nosičů,
> d) nepřetržité poskytování informací o relevantních detekovaných kybernetických bezpečnostních událostech a včasné varování relevantních osob a
> e) pravidelnou a bezodkladnou aktualizaci nástrojů pro nepřetržitou a automatickou ochranu před škodlivým kódem a dalších detekčních nástrojů a jejich pravidel.

Překlad do Microsoft 365 a Azure

- Pošta v Defender for Office 365, stanice v Defender for Business, servery v Defender for Servers, automatické spouštění blokuje Intune. Upozornění na incidenty určeným osobám i mimo pracovní dobu.

Zjištěno	Stav	Mezera
Stanice jsou chráněné a automatické spouštění blokované, upozornění ale chodí jen do sdílené schránky IT. ERP servery mají jen vestavěný antivirus mimo konzoli a RDP otevřené z internetu.	Částečně	M-05, M-06, M-08

§ 9 odst. 2 — zaznamenávání událostí

> **§ 9 odst. 2 vyhlášky č. 410/2025 Sb.**
>
> (2) Povinná osoba za účelem detekce kybernetických bezpečnostních událostí zaznamenává
> a) bezpečnostní a relevantní provozní události detekované podle odstavce 1 a bezpečnostní a relevantní provozní události technických aktiv na základě svých bezpečnostních potřeb a
> b) u událostí podle písmene a) následující informace o události:
> 1. datum a čas, včetně specifikace časového pásma,
> 2. typ činnosti,
> 3. jednoznačnou identifikaci technického aktiva a identifikaci účtu původce a
> 4. úspěšnost nebo neúspěšnost činnosti.

Překlad do Microsoft 365 a Azure

- Entra ID, auditní log Microsoft 365, Defender a události Windows ze serverů v Log Analytics. Záznam nese čas v UTC, typ činnosti, zařízení, účet a výsledek.

Zjištěno	Stav	Mezera
Auditní log Microsoft 365 je zapnutý a události obou ERP serverů se sbírají do Log Analytics. Záznamy obsahují všechny údaje podle písm. b).	Splněno	—

§ 9 odst. 3 — doba uchování záznamů

> **§ 9 odst. 3 vyhlášky č. 410/2025 Sb.**
>
> (3) Povinná osoba uchovává záznamy bezpečnostních a relevantních provozních událostí po dobu, kterou si stanoví na základě svých bezpečnostních potřeb.

Překlad do Microsoft 365 a Azure

- Dobu stanoví organizace, vyhláška 410/2025 ji nepředepisuje. 18 měsíců platí jen pro vyšší povinnosti.
- Retence Log Analytics na stanovenou dobu a Entra ID do Log Analytics přes nastavení diagnostiky. Auditní log nad 180 dní vyžaduje vyšší licenci auditu nebo export.

Zjištěno	Stav	Mezera
Dobu uchování organizace nestanovila. Platí jen výchozí retence: Entra ID 30 dní, auditní log Microsoft 365 180 dní, Log Analytics 30 dní.	Mezera	M-07

4.5 § 10 a 14 vyhlášky, § 15 a 16 zákona — řešení incidentů a hlášení

§ 10 písm. b), d) až f) — posuzování a hlášení incidentů

> **§ 10 písm. b), d) až f) vyhlášky č. 410/2025 Sb.**
>
> Povinná osoba při řešení kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
> …
> b) vytvoří metodiku pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, včetně posuzování významnosti dopadu kybernetického bezpečnostního incidentu v souladu s § 14,
> …
> d) zajistí posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů v souladu s metodikou podle písmene b),
> e) zajistí hlášení kybernetického bezpečnostního incidentu s významným dopadem podle § 15 zákona,
> f) zajistí vytvoření závěrečné zprávy o vyřešení kybernetického bezpečnostního incidentu s významným dopadem podle § 16 zákona.

Překlad do Microsoft 365 a Azure

- Metodiku stanoví organizace. V portálu Microsoft Defender ji nese řešitel, klasifikace a značka s výsledkem posouzení, závěrečnou zprávu podloží časová osa incidentu.

Zjištěno	Stav	Mezera
Metodika posuzování ani postup hlášení neexistuje. U žádného z 38 incidentů za 90 dní není záznam o posouzení významnosti.	**Mezera**	M-08

§ 14 odst. 1 a 2 — významnost dopadu incidentu

§ 14 odst. 1 a 2 vyhlášky č. 410/2025 Sb.

(1) Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví
a) únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem, v jehož důsledku ještě není ohrožen život nebo zdraví osob nebo schopnost povinné osoby dostát svým závazkům,
b) oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů zohledňující zejména
1. provozní dopad kybernetického bezpečnostního incidentu na povinnou osobu a její schopnost poskytovat regulovanou službu,
2. množství uživatelů regulované služby a jiných orgánů a osob zasažených kybernetickým bezpečnostním incidentem,
3. časové, lidské a technické zdroje, které jsou potřebné k obnově poskytování zasažené regulované služby,
4. typ a umístění aktiv dotčených kybernetickým bezpečnostním incidentem,
5. citlivost informací a dat zasažených kybernetickým bezpečnostním incidentem a újmu, jakou může narušení bezpečnosti těchto informací a dat způsobit povinné osobě nebo jinému orgánu nebo osobě, a
6. přímou příčinu kybernetického bezpečnostního incidentu, je-li povinné osobě známo, zda se jedná o lidskou chybu, technickou závadu nebo úmyslné jednání.
(2) Dopad kybernetického bezpečnostního incidentu na poskytování regulované služby je považován za významný, pokud
a) přesáhne povinnou osobou stanovenou únosnou míru újmy způsobenou kybernetickým bezpečnostním incidentem podle odstavce 1 písm. a) a současně
b) je oblast pro posouzení významnosti dopadu podle odstavce 1 písm. b) posouzena jako významná.

Překlad do Microsoft 365 a Azure

- Únosnou míru újmy a oblasti stanoví organizace, například hodiny výpadku výroby.

  V Defender je vést jako povinné značky incidentu, podklady pro body 1 až 6 dají dotčená zařízení, účty, prostředky a klasifikace.

Zjištěno	Stav	Mezera
Únosnou míru újmy ani oblasti posouzení organizace nestanovila, významnost dopadu proto nejde posoudit.	**Mezera**	M-08

§ 15 odst. 2 a 3 — hlášení Národnímu CERT podle zákona

§ 15 odst. 2 a 3 zákona č. 264/2025 Sb.

(2) Poskytovatel regulované služby v režimu nižších povinností je povinen hlásit národnímu týmu koordinace a zvládání kybernetických bezpečnostních incidentů, událostí a hrozeb (dále jen „Národní CERT“) postupem podle § 16 kybernetické bezpečnostní incidenty, které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru, mají významný dopad na poskytování regulované služby a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění.
(3) Významný dopad na poskytování regulované služby má kybernetický bezpečnostní incident, který poskytovateli regulované služby způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční ztráty nebo způsobil nebo může způsobit jiným osobám značnou újmu. Způsob vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby poskytovatelem regulované služby v režimu nižších povinností stanoví Úřad vyhláškou.

Překlad do Microsoft 365 a Azure

- Hlásí se jen incident, který splní všechny čtyři podmínky odst. 2, významný dopad se posuzuje podle § 14 vyhlášky. Podmínky vést u incidentu jako značky, adresátem je Národní CERT.

Zjištěno	Stav	Mezera
Incidenty nenesou informaci o stanoveném rozsahu, původu ani úmyslném zavinění a kdo hlášení podává, určeno není.	**Mezera**	M-08

§ 16 odst. 1, 3 a 4 — lhůty a způsob hlášení podle zákona

§ 16 odst. 1, 3 a 4 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.

...

(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,

b) na výzvu Úřadu nebo Národního CERT průběžnou zprávu o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu a

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.

(4) Poskytovatel regulované služby hlásí kybernetické bezpečnostní incidenty včetně dobrovolných hlášení podle tohoto zákona prostřednictvím Portálu Úřadu. Nelze-li využít Portálu Úřadu, poskytovatel regulované služby v režimu vyšších povinností zašle hlášení na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do datové schránky Úřadu, a poskytovatel regulované služby v režimu nižších povinností zašle hlášení na adresu elektronické pošty Národního CERT určenou pro příjem hlášení kybernetických bezpečnostních incidentů, nebo do datové schránky Národního CERT.

Překlad do Microsoft 365 a Azure

- Hlásí se jen incidenty s významným dopadem, u každého proto běží 24 hodin na prvotní hlášení a 72 hodin na oznámení od zjištění, 30 dní na závěrečnou zprávu od oznámení.
- Upozornění z Defender určeným osobám i mimo pracovní dobu, čas zjištění a hlášení v incidentu. Hlásit přes Portál Úřadu, náhradně e-mailem nebo datovou schránkou Národního CERT.

Zjištěno	Stav	Mezera
Upozornění chodí do sdílené schránky IT, kterou mimo pracovní dobu nikdo nesleduje. Lhůty nic nehlídá a náhradní kontakt na Národní CERT organizace nemá.	**Mezera**	M-08

4.6 § 11 až 13 — síť, aplikační bezpečnost, kryptografie

§ 11 — bezpečnost komunikační sítě

> **§ 11 vyhlášky č. 410/2025 Sb.**
>
> Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to zejména jejího síťového perimetru,
> a) zajistí segmentaci komunikační sítě, včetně oddělení provozního a zálohovacího prostředí,
> b) omezí odchozí a příchozí komunikaci na perimetru komunikační sítě na dobu nezbytně nutnou pro řádné zajištění poskytování regulované služby,
> c) užívá aktuálně odolné a bezpečné komunikační protokoly,
> d) v případě užití vzdáleného připojení do interní komunikační sítě nebo vzdálené správy technických aktiv regulované služby
> 1. omezí tato připojení na nezbytně nutná,
> 2. zavede bezpečnostní opatření, která zajistí důvěrnost a integritu těchto vzdálených připojení a vzdálené správy, a
> 3. má přehled o uživatelích a administrátorech, kteří tato vzdálená připojení nebo vzdálenou správu užívají.

Překlad do Microsoft 365 a Azure

- Podsítě s pravidly NSG, zálohy v trezoru mimo virtuální síť, odchozí provoz jen na potřebné cíle.
- RDP z internetu zavřít, správa přes Azure Bastion nebo přístup just-in-time z Defender for Servers Plan 2, který port otevře jen na dobu správy. Kdo smí spravovat, určují role v Azure.

Zjištěno	Stav	Mezera
Podsítě aplikace a databáze jsou oddělené, zálohy leží mimo síť a VPN do závodu používá IKEv2 s AES-256. RDP aplikačního serveru je ale otevřené z internetu pod sdíleným účtem a odchozí provoz omezený není.	Částečně	M-05

§ 12 — aplikační bezpečnost

> **§ 12 vyhlášky č. 410/2025 Sb.**
>
> Povinná osoba při zajišťování aplikační bezpečnosti regulované služby
> a) zajistí bezodkladné aplikování schválených bezpečnostních aktualizací vydaných pro technická aktiva,
> b) u technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována
> 1. vede jejich evidenci,
> 2. zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti, a
> 3. omezí jejich komunikaci v komunikační síti na nezbytně nutnou,
> c) provádí pravidelné skenování zranitelností relevantních technických aktiv a aplikuje přiměřená bezpečnostní opatření na základě zjištěných výsledků.

Překlad do Microsoft 365 a Azure

- Stanice: aktualizační okruhy Intune a správa zranitelností v Defender for Business. Servery: Azure Update Manager s plánem instalace a skenování v Defender for Servers.

Zjištěno	Stav	Mezera
Stanice se aktualizují i skenují automaticky a nepodporovaný systém žádná nemá. ERP servery aktualizuje externí správce ručně, naposledy před čtyřmi měsíci, a zranitelnosti na nich nikdo neskenuje.	Částečně	M-06, M-10

§ 13 odst. 1 — kryptografické algoritmy

> **§ 13 odst. 1 vyhlášky č. 410/2025 Sb.**
>
> (1) Povinná osoba při zajištění bezpečnosti technických aktiv a jejich komunikace
> a) používá aktuálně odolné kryptografické algoritmy,
> b) prosazuje bezpečné nakládání s kryptografickými algoritmy a
> c) zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Národním úřadem pro kybernetickou a informační bezpečnost.

Překlad do Microsoft 365 a Azure

- Přenos TLS 1.2 a vyšší, data v klidu AES-256, BitLocker z Intune, VPN se zásadou IPsec podle doporučení Úřadu ke kryptografickým algoritmům.

Zjištěno	Stav	Mezera
Microsoft 365 a Azure šifrují přenos i data v klidu, BitLocker je vynucený na všech stanicích. Zásadu IPsec VPN s IKEv2, AES-256 a SHA-256 organizace porovnala s doporučením Úřadu.	Splněno	—

§ 13 odst. 2 písm. a) — bezpečná komunikace a e-mail

> **§ 13 odst. 2 písm. a) vyhlášky č. 410/2025 Sb.**
>
> (2) Povinná osoba zajišťuje bezpečnou
> a) hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace, a

Překlad do Microsoft 365 a Azure

- Teams šifruje hovory, schůzky i zprávy. Pošta: SPF, podpis DKIM a DMARC s politikou quarantine nebo reject.

Zjištěno	Stav	Mezera
Teams i pošta šifrují přenos. DKIM je vypnutý a záznam DMARC chybí, podvržené zprávy jménem organizace proto příjemci neodmítnou.	Částečně	M-09

5. Mezery

Dvě mezery v plném znění: jediná kritická a mezera v hlášení, ve kterém se nižší povinnosti od vyšších liší nejvíc. Všech 10 je v registru mezer v příloze.

5.1 M-05 — Na ERP server se správci přihlašují přes RDP z internetu jen heslem

Vlastnost	Hodnota
Ustanovení	§ 7 odst. 1 písm. a) a b), § 8 odst. 1, § 8 odst. 2, § 8 odst. 3 a 4, § 8 odst. 5, § 9 odst. 1, § 11
Priorita	**Kritická**
Pracnost	Nízká

5.1.1 Zjištěný stav

Pravidlo NSG aplikačního serveru ERP povoluje port 3389 z celého internetu. Externí i interní správci se hlásí vestavěným účtem správce jen heslem a server za 30 dní zaznamenal přes 41 000 neúspěšných pokusů o přihlášení.

Ověření: pravidla NSG otevřená z internetu (Azure Resource Graph)

```
resources
| where type =~ "microsoft.network/networksecuritygroups"
| mv-expand r = properties.securityRules
| where r.properties.direction == "Inbound" and r.properties.access == "Allow"
    and tostring(r.properties.sourceAddressPrefix) in ("*", "Internet")
| project nsg = name, port = tostring(r.properties.destinationPortRange)
```

5.1.2 Dopad

Server, ze kterého se plánuje výroba a expedice, je vystavený útokům na hesla z celého internetu. Kdo heslo získá, ovládne ERP. Činnost pod sdíleným účtem nejde přiřadit konkrétnímu člověku.

5.1.3 Doporučení

- Hned odebrat pravidlo NSG pro port 3389 z internetu i veřejnou adresu serveru.
- Správu vést přes Azure Bastion, na servery se hlásit jmennými účty Entra ID s vícefaktorovou autentizací z Conditional Access.

- Vestavěný účet správce ponechat jen pro obnovu, s náhodným heslem alespoň 17 znaků v trezoru podle § 8 odst. 4 písm. a) bod 2.
- Odchozí provoz serverů omezit pravidly NSG na potřebné cíle.

5.2 M-08 — Chybí posouzení významnosti incidentu a postup hlášení Národnímu CERT

Vlastnost	Hodnota
Ustanovení	§ 9 odst. 1, § 10 písm. b), d) až f), § 14 odst. 1 a 2, zákon § 15 odst. 2 a 3, zákon § 16 odst. 1, 3 a 4
Priorita	**Vysoká**
Pracnost	Střední

5.2.1 Zjištěný stav

Za 90 dní vzniklo v portálu Microsoft Defender 38 incidentů, upozornění chodí do sdílené schránky IT. U žádného nejde zjistit, zda se projevil ve stanoveném rozsahu, jaký měl dopad a kdo rozhodl, že se nehlásí. Únosnou míru újmy ani oblasti posouzení podle § 14 vyhlášky organizace nestanovila.

Ověření: incidenty za 90 dní s řešitelem, klasifikací a značkami (Microsoft Graph)

```
Connect-MgGraph -Scopes "SecurityIncident.Read.All"
Get-MgSecurityIncident -All `
    -Filter "createdDateTime ge 2026-06-24T00:00:00Z" |
  Select-Object CreatedDateTime, DisplayName, Severity, Status,
    AssignedTo, Classification, CustomTags
```

5.2.2 Dopad

Organizace nepozná, který incident má hlásit. Lhůta 24 hodin od zjištění může uplynout dřív, než incident někdo otevře, a u hlášeného incidentu nejde doložit oznámení do 72 hodin ani závěrečnou zprávu do 30 dní.

5.2.3 Doporučení

- Organizace stanoví únosnou míru újmy a oblasti posouzení podle § 14 vyhlášky a určí, kdo incidenty přebírá, posuzuje a hlásí, včetně zástupce.

- Upozornění na incidenty vysoké a střední závažnosti posílat těmto osobám, ne do sdílené schránky.
- Aktiva ze stanoveného rozsahu označit značkami, u incidentu zapsat čtyři podmínky § 15 odst. 2 zákona a rozhodnutí o hlášení s časem.
- Kontakty pro Portál Úřadu a náhradní kanály Národního CERT mít v postupu i mimo Microsoft 365.

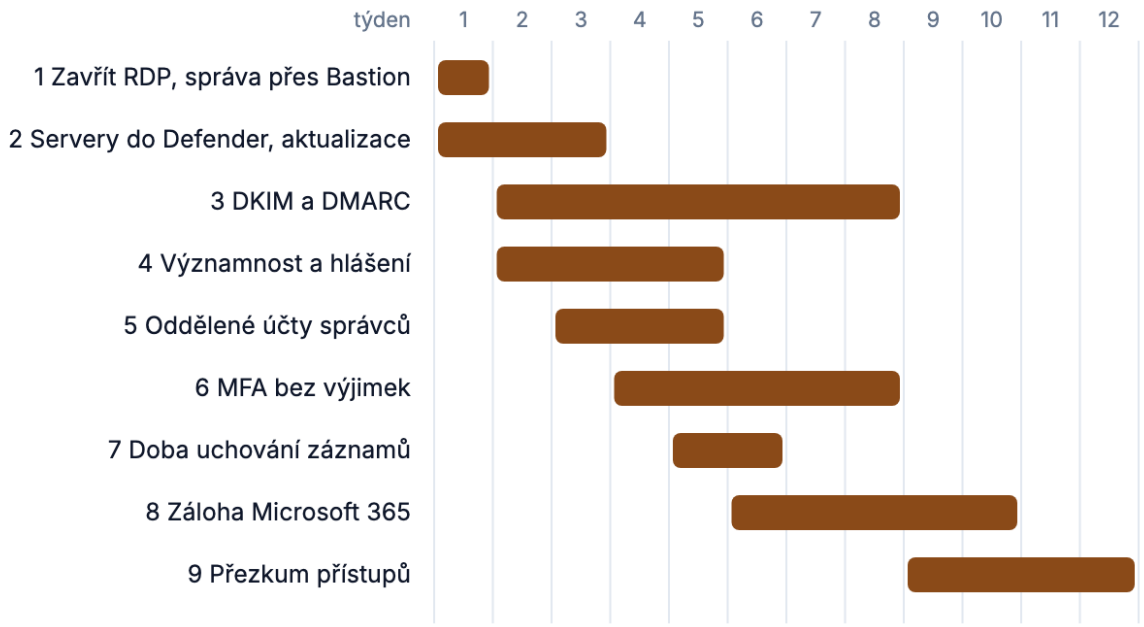
Hlášení incidentu s významným dopadem podle § 16 zákona

Krok	Lhůta	Obsah
Prvotní hlášení	do 24 hodin po zjištění	identifikační údaje, základní údaje o incidentu, zda jde o nezákonný zásah a zda může mít přeshraniční dopad
Oznámení	do 72 hodin po zjištění	aktualizace, prvotní posouzení, dopad a indikátory kompromitace
Průběžná zpráva	na výzvu Úřadu nebo Národního CERT	podstatné změny stavu zvládání incidentu
Závěrečná zpráva	do 30 dní od oznámení	vyřešení incidentu; trvá-li, průběžná zpráva a závěrečná do 30 dní od vyřešení

6. Roadmapa

Pořadí je podle priority a závislostí: kritická mezera první, posouzení významnosti a hlášení hned potom, přezkum přístupů až nad uklizenými rolemi a účty.

Harmonogram (týdny)



Kroky roadmapy, pracnost kroku je nejvyšší pracnost z jeho mezer

Krok	Obsah	Mezery	Pracnost
1	RDP z internetu zavřít, Azure Bastion, účty Entra ID na serverech	M-05	Nízká
2	Defender for Servers, Azure Update Manager s plánem instalace	M-06, M-10	Nízká
3	DKIM a DMARC ve sledování, pak politika quarantine	M-09	Nízká
4	Únosná míra újmy, odpovědné osoby, značky a upozornění v Defender	M-08	Střední
5	Oddělené účty správců s nejužší rolí, i pro externího správce	M-02	Střední
6	Servisní účty na certifikát, osobní účty v expedici, bez výjimek	M-01	Střední
7	Stanovit dobu uchování, retence Log Analytics, Entra ID do něj	M-07	Nízká
8	Záloha Microsoft 365 a konfigurace tenantu, test obnovy	M-04	Střední
9	Čtvrtletní přezkum rolí, skupin a hostů, seznam pro odchody	M-03	Nízká

7. Přílohy

7.1 Registr mezer

ID	Mezera	Ustanovení	Priorita	Pracnost
M-01	Servisní účty a sdílený účet expedice se přihlašují jen heslem	§ 7 odst. 1 písm. a) a b), § 8 odst. 2, § 8 odst. 3 a 4	Vysoká	Střední
M-02	Správci nemají oddělené účty, globálního správce mají trvale i hosté externího správce	§ 7 odst. 1 písm. a) a b)	Vysoká	Střední
M-03	Přístupy nikdo nepřezkoumává a po odchodu zůstávají aktivní	§ 7 odst. 1 písm. d), § 7 odst. 1 písm. e) a f)	Střední	Nízká
M-04	Data a konfigurace Microsoft 365 se nezálohují	§ 6 písm. c)	Vysoká	Střední
M-05	Na ERP server se správci přihlašují přes RDP z internetu jen heslem	§ 7 odst. 1 písm. a) a b), § 8 odst. 1, § 8 odst. 2, § 8 odst. 3 a 4, § 8 odst. 5, § 9 odst. 1, § 11	Kritická	Nízká
M-06	ERP servery jsou mimo detekci i skenování zranitelností	§ 9 odst. 1, § 12	Vysoká	Nízká
M-07	Doba uchování záznamů není stanovená	§ 9 odst. 3	Střední	Nízká
M-08	Chybí posouzení významnosti incidentu a postup hlášení Národnímu CERT	§ 9 odst. 1, § 10 písm. b), d) až f), § 14 odst. 1 a 2, zákon § 15 odst. 2 a 3, zákon § 16 odst. 1, 3 a 4	Vysoká	Střední
M-09	Doména nemá DMARC a pošta není podepsaná DKIM	§ 13 odst. 2 písm. a)	Střední	Nízká
M-10	Aktualizace ERP serverů se instalují ručně a pozdě	§ 12	Střední	Nízká

7.2 Důkazní balík

Doklady s datem a zdrojem, které jde kdykoli zopakovat. Doklady k mezerám vzniknou po jejich odstranění.

Doklad	Odkud se exportuje	Ustanovení
Politiky Conditional Access, účty a jejich metody ověření	Entra ID, Microsoft Graph	§ 8 odst. 2 až 4

Doklad	Odkud se exportuje	Ustanovení
Role Entra ID a Azure, hosté, identity aplikací, přezkumy	Entra ID, Azure, Microsoft Graph	§ 7 odst. 1
Pravidla shody a ochrany aplikací	Intune	§ 7 odst. 1 písm. c)
Ochrana, zranitelnosti a aktualizace stanic a serverů	portál Microsoft Defender, Intune, Azure Update Manager	§ 9 odst. 1, § 12
Retence záznamů a nastavení diagnostiky	Log Analytics, Entra ID, Purview	§ 9 odst. 2 a 3
Incidenty se značkami a rozhodnutím o hlášení	portál Microsoft Defender, Microsoft Graph	§ 10, zákon § 15 a 16
Pravidla NSG, přístup přes Bastion, zásada IPsec	Azure Resource Graph	§ 11, § 13 odst. 1
Nastavení záloh a protokol testu obnovy	Azure Backup, záloha Microsoft 365	§ 6 písm. c)
Záznamy SPF, DKIM a DMARC	DNS, Defender for Office 365	§ 13 odst. 2 písm. a)

7.3 Povinnosti mimo rozsah

Nejde o mezery analýzy. Organizace je zajišťuje a dokládá mimo Microsoft 365 a Azure, cloud k nim dodá nanejvýš podklad.

Ustanovení	Povinnost	Podklad z Microsoft 365 a Azure
§ 3 odst. 1 písm. a)	opatření přiměřená potřebám, řízení rizik	Secure Score, doporučení Defender for Cloud
§ 3 odst. 2	přehled bezpečnostních opatření	tento report, viz níže
§ 3 odst. 3	bezpečnostní politika a dokumentace	Conditional Access a Intune vynucují její pravidla
§ 3 odst. 4	pravidla pro technická aktiva	inventář zařízení v Intune a Defender
§ 3 odst. 5	smlouvy s dodavateli podle přílohy č. 2	smluvní podmínky a auditní zprávy Microsoftu
§ 3 odst. 6	požadavky při akvizici, vývoji a údržbě	—
§ 4 a 5	vrcholné vedení, lidské zdroje a školení	—
§ 6 písm. a) a b)	priorita a postupy obnovy, odpovědnost	nastavení záloh, protokol testu obnovy
§ 7 odst. 2	fyzická bezpečnost	auditní zprávy Microsoftu k datovým centrům
§ 10 písm. a)	oznamování neobvyklého chování	hlášení podezřelé zprávy z Outlooku
§ 13 odst. 2 písm. b)	nouzová komunikace v organizaci	—, nemá záviset na Microsoft 365

Ustanovení	Povinnost	Podklad z Microsoft 365 a Azure
zákon § 12	stanovený rozsah a evidence aktiv	inventář Intune a Defender, značky v Azure
§ 3 až 13	opatření pro výrobní linky, síť závodu a aplikaci ERP	—

§ 3 odst. 2 vyhlášky č. 410/2025 Sb.

(2) Povinná osoba
a) stanoví přehled bezpečnostních opatření podle přílohy č. 1 k této vyhlášce, který obsahuje přehled všech bezpečnostních opatření, která
1. byla povinnou osobou zavedena, včetně popisu jejich zavedení,
2. budou povinnou osobou zavedena, včetně termínů pro jejich zavedení, priority jejich zavedení a určení osoby odpovědné za jejich zavedení, a
3. nebyla zavedena, včetně odůvodnění jejich nezavedení,
b) provede a dokumentuje alespoň jednou ročně aktualizaci přehledu bezpečnostních opatření, včetně vyhodnocení účinnosti zavedených bezpečnostních opatření,
c) uchovává jednotlivé přehledy bezpečnostních opatření a jejich aktualizace alespoň po dobu 4 let.

Co report dodá do přehledu bezpečnostních opatření, který si organizace vede sama

§ 3 odst. 2	Z reportu	Doplní organizace
písm. a) bod 1, zavedená opatření	ustanovení ve stavu Splněno se zjištěným nastavením	—
písm. a) bod 2, opatření k zavedení	registr mezer, priorita a pořadí z roadmapy	termín a odpovědnou osobu
písm. a) bod 3, nezavedená opatření	—	odůvodnění nezavedení
písm. b), roční aktualizace	opakování analýzy a důkazního balíku	vyhodnocení účinnosti