PERMETRIA

UKÁZKOVÁ ZPRÁVA

```
$ audit --scope critical --read-only
```

Bezpečnostní audit Microsoft Entra ID

Kritická úroveň: privilegovaný přístup a autentizace

12 kontrolních bodů · ověření přes Microsoft Graph API (pouze čtení)

VÝSLEDEK KONTROL



KLIENT
Ukázkový tenant (demo prostředí)

DATUM AUDITU
20. 9. 2026

VYHOTOVENO
28. 9. 2026

SHRNUTÍ PRO VEDENÍ

Celkový stav zabezpečení

Audit ověřil 12 kontrolních bodů s nejvyšším dopadem na bezpečnost tenantu: privilegované role, vícefaktorové ověření a základní ochranné politiky. Kontroly proběhly automatizovaně přes Microsoft Graph API v režimu pouze pro čtení, body vyžadující lidský úsudek byly ověřeny ručně.

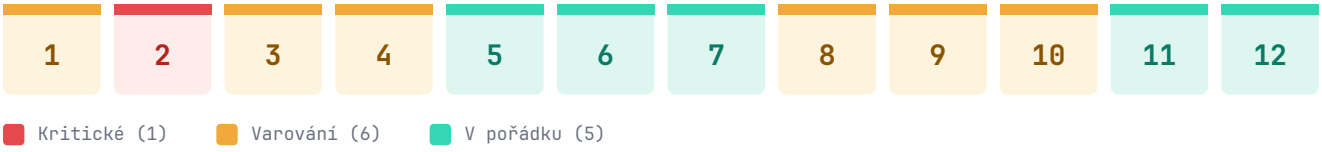
CELKOVÉ RIZIKO

Vysoké

Tenant má kritický nedostatek v ochraně privilegovaných účtů: žádný z 12 administrátorů nemá registrované MFA. Náprava je technicky nenáročná a výrazně sníží riziko převzetí kontroly nad celým tenantem.

1	6	5	2
KRITICKÝCH	VAROVÁNÍ	V POŘÁDKU	OVĚŘENO RUČNĚ

PŘEHLED VŠECH 12 KONTROL



Klíčová zjištění

1 **12 privilegovaných účtů bez MFA**

U 12 účtů s administrátorskou rolí (z toho 9 s rolí Global Administrator) není registrována žádná metoda vícefaktorového ověření. Kompromitace jediného hesla tak může znamenat plnou kontrolu nad tenantem.

2 **Příliš mnoho trvalých administrátorů**

V tenantu je 9 Global Administrátorů (doporučeno 2–4) a 14 trvalých přiřazení rolí. Privileged Identity Management se nevyužívá, oprávnění jsou aktivní nepřetržitě.

3 **Základní ochrana stojí jen na Security Defaults**

Security Defaults pokrývají základ (MFA, legacy autentizace), ale v tenantu není žádná Conditional Access politika. Chybí kontrola zařízení, lokací a rizika přihlášení i možnost granulárních výjimek.

PODROBNÁ ZJIŠTĚNÍ

Výsledky jednotlivých kontrol

KRITICKÁ ZJIŠTĚNÍ · 1

02 MFA pro privilegované role

KRITICKÉ

ZJIŠTĚNÍ

U 12 účtů s privilegovanou rolí (9× Global Administrator, dále Privileged Role Administrator, Exchange Administrator a User Administrator) není registrována žádná metoda vícefaktorového ověření. Security Defaults registraci MFA vyžadují, u těchto účtů ji ale dosud nikdo neprovedl. Úplný seznam je v příloze A.

DOPORUČENÍ

Zaregistrovat MFA (Microsoft Authenticator nebo FIDO2 klíč) u všech administrátorských účtů. Pro nouzové účty použít FIDO2 klíče uložené offline.

VAROVÁNÍ · 6

01 Počet Global Administrátorů

VAROVÁNÍ

ZJIŠTĚNÍ

V tenantu je 9 účtů s rolí Global Administrator (doporučeno 2–4), z toho 3 nouzové. Mezi ostatními jsou účty, jejichž název naznačuje zastaralost (Admin Old) nebo servisní použití (SVC Backup).

DOPORUČENÍ

Snížit počet na 2–4 personální účty a 2 nouzové. Zastaralé účty odebrat, servisní účet nahradit aplikací s minimálními oprávněními.

03 Nouzové (break-glass) účty

RUČNĚ OVĚŘENO

VAROVÁNÍ

ZJIŠTĚNÍ

Ručně ověřeno: identifikovány 3 účty s charakterem nouzového přístupu. Jsou cloud-only, ale nemají registrovanou silnou metodu (FIDO2), názvosloví je nejednotné a nad jejich přihlášením není nastaven alert.

DOPORUČENÍ

Ponechat 2 nouzové účty s jednotným pojmenováním, zabezpečit je FIDO2 klíči a nastavit okamžitý alert při každém přihlášení.

04 Privileged Identity Management (PIM)

VAROVÁNÍ

ZJIŠTĚNÍ

Evidováno 14 trvalých přiřazení rolí a 0 přiřazení typu eligible. Administrátorská oprávnění jsou tak aktivní nepřetržitě, nikoli jen v době potřeby.

DOPORUČENÍ

Nasadit PIM (vyžaduje Entra ID P2), převést administrátorské role na eligible s časově omezenou aktivací a odůvodněním.

08 Compliant / hybrid-joined zařízení

VAROVÁNÍ

ZJIŠTĚNÍ

Žádná politika nevyžaduje pro přístup k citlivým aplikacím compliant nebo hybrid-joined zařízení.

DOPORUČENÍ

Po nasazení správy zařízení (Intune) vyžadovat compliant zařízení minimálně pro administrátory a citlivé aplikace (vyžaduje Entra ID P1).

09 Blokování rizikových lokací — VAROVÁNÍ

ZJIŠTĚNÍ
Nebyla nalezena politika blokující přihlášení z rizikových či neobvyklých lokací a anonymizovaných sítí.
DOPORUČENÍ
Definovat důvěryhodné lokace a blokovat přístup ze zemí, odkud organizace nikdy nepracuje (vyžaduje Entra ID P1).

10 Identity Protection – risk policies — VAROVÁNÍ

ZJIŠTĚNÍ
Nejsou nakonfigurovány politiky reagující na riziko uživatele ani přihlášení. Funkce vyžaduje licenci Entra ID P2.
DOPORUČENÍ
Při dostupné licenci P2 vynutit MFA při středním riziku přihlášení a reset hesla při vysokém riziku uživatele.

V POŘÁDKU · 5

05 MFA přes Conditional Access — V POŘÁDKU

ZJIŠTĚNÍ
Žádná Conditional Access politika MFA nevyžaduje, vícefaktorové ověření však vynucují zapnuté Security Defaults.
DOPORUČENÍ
Pro granulární řízení (výjimky, síla metod, kontext) doporučujeme přechod na Conditional Access (vyžaduje Entra ID P1).

06 Blokování legacy autentizace — V POŘÁDKU

ZJIŠTĚNÍ
Dedikovaná politika neexistuje, legacy protokoly (POP, IMAP, SMTP AUTH) však blokují zapnuté Security Defaults.
DOPORUČENÍ
Pro auditovatelnost a řízené výjimky doporučujeme politiku Conditional Access (vyžaduje Entra ID P1).

07 Security Defaults — V POŘÁDKU

ZJIŠTĚNÍ
Security Defaults jsou zapnuté a žádná Conditional Access politika neexistuje, takže nevzniká konflikt konfigurací.
DOPORUČENÍ
Základní ochrana je zajištěna. Pro produkční provoz doporučujeme přechod na Conditional Access.

11 Self-Service Password Reset (SSPR) — V POŘÁDKU
RUČNĚ OVĚŘENO

ZJIŠTĚNÍ
Ručně ověřeno: SSPR je zapnuto pro všechny uživatele a vyžaduje dvě metody ověření.
DOPORUČENÍ
Bez akce. Pravidelně přezkoumávat povolené metody ověření.

12 Vlastní (custom) role — V POŘÁDKU

ZJIŠTĚNÍ
V tenantu nejsou definovány žádné vlastní role.
DOPORUČENÍ
Bez akce. Při budoucím vytváření rolí dodržet princip minimálních oprávnění.

AKČNÍ PLÁN

Doporučený postup nápravy

Kroky jsou seřazeny podle poměru přínosu a náročnosti. První fáze cílí na nejvyšší rizika a její hlavní kroky nevyžadují další licence.

FÁZE 1

Okamžitě

do 48 hodin

- Zaregistrovat MFA u všech 12 privilegovaných účtů
- Odebrat zastaralé účty (např. Admin Old) a nepotřebná přiřazení Global Administrator
- Ověřit dostupnost nouzových účtů (FIDO2 klíč uložený offline)

FÁZE 2

Krátkodobě

do 4 týdnů

- Snížit počet Global Administrátorů na 2–4 a 2 nouzové účty (FIDO2)
- Nasadit PIM a převést role na eligible s časově omezenou aktivací
- Zavést Conditional Access s vyžadováním MFA pro všechny uživatele
- Nastavit alert na přihlášení nouzových účtů

FÁZE 3

Střednědobě

do 3 měsíců

- Definovat důvěryhodné lokace a blokovat rizikové země
- Vyžadovat compliant zařízení pro citlivé aplikace
- Zapnout risk-based politiky Identity Protection (P2)
- Přejít ze Security Defaults na Conditional Access
- Pokračovat dalšími kontrolami: hosté, aplikace, Access Reviews

DALŠÍ KROK

Kompletní audit: 50 kontrolních bodů

Tato zpráva pokrývá 12 nejkritičtějších bodů. Kompletní audit navíc prověří hosty a externí spolupráci, souhlasy aplikací, service principaly, monitoring a provozní hygienu tenantu a zahrnuje konzultaci nálezů a plán nápravy. Napište mi a společně projdeme, co by audit ve vašem prostředí pokryl.

permetria.cz · martin.pavlicek@permetria.cz

PŘÍLOHA A

Privilegované účty bez registrované MFA

Seznam účtů, u kterých kontrola bodu 02 nenašla žádnou registrovanou metodu vícefaktorového ověření.

#	ÚČET (UPN)	ROLE	POZNÁMKA
1	audit.user_example.com#EXT#@demo-tenant.onmicrosoft.com	Global Administrator	externí (guest)
2	jan.novak@demo-tenant.onmicrosoft.com	Global Administrator	
3	richard.vesely@demo-tenant.onmicrosoft.com	Global Administrator	
4	admin.old@demo-tenant.onmicrosoft.com	Global Administrator	zastaralý (dle názvu)
5	admin@demo-tenant.onmicrosoft.com	Global Administrator	
6	svc.backup@demo-tenant.onmicrosoft.com	Global Administrator	servisní (dle názvu)
7	breakglass01@demo-tenant.onmicrosoft.com	Global Administrator	nouzový (dle názvu)
8	BreakGlass-Admin01@demo-tenant.onmicrosoft.com	Global Administrator	nouzový (dle názvu)
9	BreakGlass-Admin02@demo-tenant.onmicrosoft.com	Global Administrator	nouzový (dle názvu)
10	martin.prochazka@demo-tenant.onmicrosoft.com	Privileged Role Administrator	
11	svc.scan2mail@demo-tenant.onmicrosoft.com	Exchange Administrator	servisní (dle názvu)
12	test.user@demo-tenant.onmicrosoft.com	User Administrator	

PŘÍLOHA B

Rozsah, metodika a hodnocení

Rozsah a postup

— Ověřeno 12 nejkritičtějších bodů z 50bodového rámce kontrol Microsoft Entra ID. Kontroly proběhly automatizovaně přes Microsoft Graph API výhradně s oprávněními ke čtení, v tenantu nebyla provedena žádná změna.

— Body, které nelze plně ověřit přes API (03 a 11), byly posouzeny ručně v administračním centru Entra. Zpráva popisuje stav v den auditu (20. 9. 2026).

Stupnice hodnocení

KRITICKÉ	Nedostatek, který může vést k převzetí účtů nebo celého tenantu. Řešit okamžitě.
VAROVÁNÍ	Odchylka od doporučených postupů se zvýšeným rizikem. Řešit v řádu týdnů.
V POŘÁDKU	Kontrola splněna. Případné doporučení se týká dalšího zlepšení, nikoli nápravy.

Omezení a licence

— Hodnocení vychází z běžně doporučovaných postupů pro Microsoft Entra ID, nejde o penetrační test ani právní posouzení souladu. Automatizovaná kontrola vidí konfiguraci, nikoli záměr organizace, proto zjištění doporučujeme před změnami prodiskutovat se správcem tenantu.

— Některá doporučení vyžadují licenci Entra ID P1 (Conditional Access) nebo P2 (PIM, Identity Protection); požadavek je u nich uveden.

O této ukázce

Zpráva vznikla nad demonstračním tenantem a ukazuje podobu výstupu, který organizace při auditu obdrží. Názvy účtů a domén jsou testovací, ručně ověřované body (03 a 11) jsou zpracovány pro účely ukázky.