BEARCLAVE

# Report z analýzy

Hardening Microsoft 365 a Azure

| | |
|---|---|
| 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

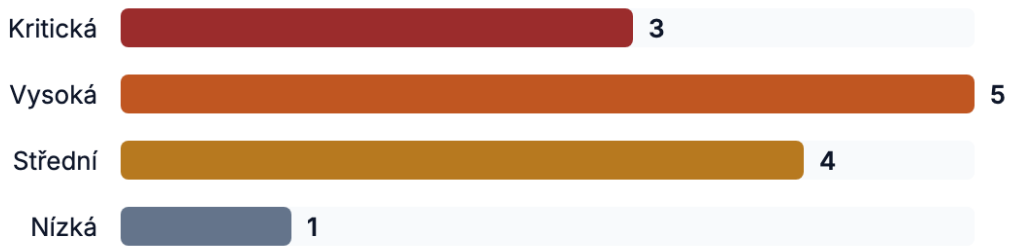
| 48 % | 9 z 13 | 6 účtů | 21 účtů |
|---|---|---|---|
| Microsoft Secure Score | nálezů exponovaných ven | trvale Global Administrator | se přihlašuje jen heslem |

Microsoft Secure Score organizace je 48 %, samotné číslo ale neříká, kde je riziko. Devět ze třinácti nálezů může útočník zneužít přímo z internetu, zbylé čtyři zhorší dopad útoku, až k němu dojde.

Nejvážnější jsou tři. Šest lidí má trvale roli Global Administrator a čte z téhož účtu poštu, 21 účtů se přihlašuje jen heslem a v Azure je z internetu dostupný vzdálený přístup na testovací server i úložiště s výkresy.

Náprava kritických a vysokých nálezů nevyžaduje nákup licencí. Doporučujeme nejdřív zavřít, co je otevřené do internetu, pak zajistit nouzový přístup a záznamy a teprve potom měnit pravidla přihlašování.

*Nálezy podle priority*



# 2. Rozsah a metoda

| Prostředí | Hodnota |
|---|---|
| Tenant | jeden tenant Microsoft 365, 280 uživatelských účtů |
| Licence | Microsoft 365 Business Premium: Entra ID P1, Intune, Defender for Business, Defender for Office 365 Plan 1 |
| Identita | hybridní, Entra Connect Sync se synchronizací hodnot hash hesel |
| Zařízení | Intune, 260 počítačů s Windows a 190 telefonů |
| Azure | jedno předplatné, 3 virtuální servery, 2 účty úložiště |
| Přístup analýzy | jen čtení: Global Reader v Entra ID, Reader na předplatném Azure |

Analýza pokrývala osm oblastí: privilegované účty, Conditional Access, ověřování, zařízení, poštu a spolupráci, Azure, aplikace a logování. Pracovalo se jen se čtením, do provozu analýza nezasahovala. Ověřovací dotazy v reportu jsou pro Microsoft Graph PowerShell a Exchange Online PowerShell.

## 2.1 Proti čemu se měřilo

- Měřítka: Microsoft Secure Score, CIS Microsoft 365 Foundations Benchmark, u Azure Defender for Cloud podle Microsoft cloud security benchmark. Doplňuje je baseline Bearclave, například kdo je ve výjimkách z politik.
- Posouzení v kontextu: co je dosažitelné z internetu, co by útočník potřeboval a jak by se zneužití projevilo.
- Typ nálezu: Exponované ven jde zneužít z internetu, stačí heslo, odkaz nebo adresa. Nedoladěné samo nikoho dovnitř nepustí, ale zhorší dopad útoku.

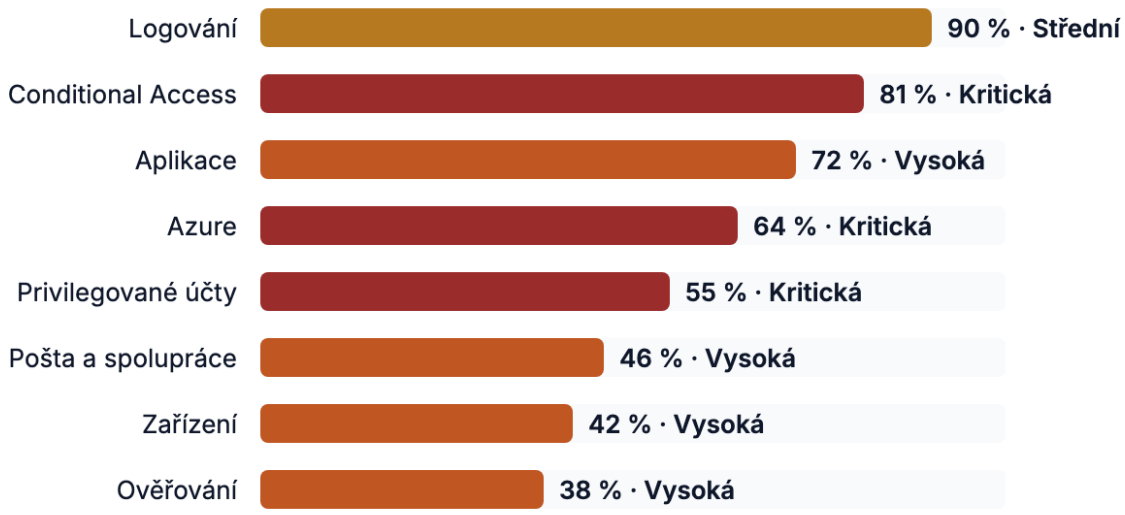
## 2.2 Co analýza není

- Penetrační test ani audit souladu — nic se aktivně nezkoušelo ani nezneužívalo.
- Implementace náprav — doporučení jsou v reportu, provedení je navazující práce.
- Vlastní aplikace organizace, lokální Active Directory nad rámec synchronizace a prostředí mimo Microsoft 365 a Azure.

## 3. Skóre a posouzení v kontextu

Skóre a riziko nejdou stejným směrem. Graf ukazuje Microsoft Secure Score podle oblasti a barvou prioritu, kterou oblasti dává posouzení v kontextu. Conditional Access má druhé nejvyšší skóre, a přesto patří mezi tři kritické oblasti.

*Microsoft Secure Score podle oblasti, barva je priorita v kontextu*




| Oblast | Skóre | Priorita | Co rozhoduje |
|---|---|---|---|
| Logování | 90 % | Střední | Záznamy Entra ID se drží jen 30 dní (N-013) |
| Conditional Access | 81 % | Kritická | Skupina výjimek vyjímá z politik 21 účtů (N-003) |
| Aplikace | 72 % | Vysoká | Aplikace s přístupem ke všem schránkám (N-011) |
| Azure | 64 % | Kritická | Veřejný kontejner a RDP z internetu (N-010) |
| Privilegované účty | 55 % | Kritická | Šest trvalých globálních správců (N-001) |
| Pošta a spolupráce | 46 % | Vysoká | Rozhoduje přeposílání ven, ne ladění prahů (N-008) |
| Zařízení | 42 % | Vysoká | Přístup z nespravovaných zařízení (N-006) |
| Ověřování | 38 % | Vysoká | Správci bez metody odolné proti phishingu (N-005) |

> Skóre oblasti je podíl bodů Microsoft Secure Score v jejích doporučeních, u Azure secure score v Defender for Cloud. Body mají různou váhu, oblasti se proto nedají zprůměrovat na celkových 48 %.

# 4. Nálezy

Tři nálezy v plném znění. Všech třináct je v registru nálezů v příloze.

## 4.1 N-001 — Šest trvalých globálních správců, dva z lokální AD

| Vlastnost | Hodnota |
|---|---|
| Oblast | Privilegované účty |
| Priorita | **Kritická** |
| Typ | Exponované ven |
| Pracnost | Střední |

### 4.1.1 Zjištěný stav

Kromě dvou nouzových účtů má roli Global Administrator trvale šest osobních účtů, včetně finančního ředitele, který ji dostal kvůli nákupu licencí, a externího správce sítě. Dva z nich jsou synchronizované z lokální Active Directory a všech šest slouží i k běžné práci s poštou. Časově omezené role (PIM) licence Entra ID P1 nezahrnuje, trvalé je proto všechno.

*Ověření: globální správci, původ účtu a licence*

```
$ga = "62e90394-69f5-4237-9190-012177145e10"  # Global Administrator
Get-MgRoleManagementDirectoryRoleAssignment -All `
    -Filter "roleDefinitionId eq '$ga'" | ForEach-Object {
  Get-MgUser -UserId $_.PrincipalId `
    -Property displayName,onPremisesSyncEnabled,assignedLicenses
} | Select-Object DisplayName, OnPremisesSyncEnabled,
    @{n="Licence"; e={$_.AssignedLicenses.Count}}
```

### 4.1.2 Dopad

Kdo ovládne lokální Active Directory, může synchronizovaným správcům nastavit heslo a od převzetí tenantu ho dělí jen druhý faktor. Stejně tak stačí jedno vylákané přihlášení kteréhokoli ze šesti účtů, protože SMS ani potvrzení v aplikaci proti podvodné stránce nechrání (N-005).

### 4.1.3 Doporučení

- Ponechat dva osobní globální správce a dva nouzové účty, ostatním dát nejmenší roli, která stačí. Finančnímu řediteli stačí Billing Administrator, externí správce sítě roli v cloudu nepotřebuje.

- Pro správu založit oddělené cloudové účty bez schránky a bez synchronizace z AD a vyžadovat pro ně v Conditional Access sílu ověření odolnou proti phishingu.
- Před odebráním rolí projít neinteraktivní přihlášení těchto účtů za 30 dní. Analýza tak našla skript, který pod účtem IT manažera zakládá uživatele.
- PIM vyžaduje Entra ID P2 pro každého, kdo má roli přiřazenou přes PIM nebo aktivace schvaluje, tady zhruba pět účtů. Zvážit až po úklidu výše.

## 4.2 N-003 — Skupina výjimek z Conditional Access, 21 účtů jen s heslem

| Vlastnost | Hodnota |
|---|---|
| Oblast | Conditional Access |
| Priorita | **Kritická** |
| Typ | Exponované ven |
| Pracnost | Vysoká |

### 4.2.1 Zjištěný stav

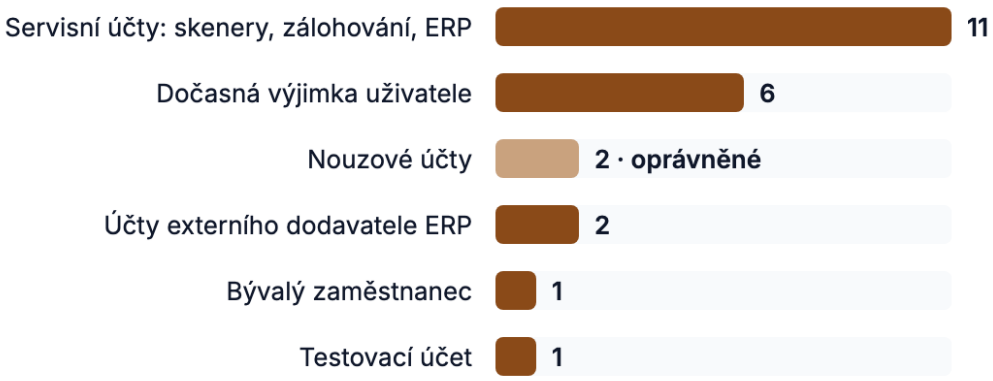
Osm z devíti politik Conditional Access vylučuje skupinu CA-Vyjimky, včetně politiky, která vyžaduje vícefaktorové ověření pro všechny uživatele. Skupina má 23 členů a žádného vlastníka, členství může měnit každý s rolí User Administrator nebo Groups Administrator a změna se nikde nehlídá. Kromě dvou nouzových účtů se všichni členové přihlašují jen heslem.

*Ověření: politiky, které skupinu vylučují, a poslední přihlášení členů*

```
$g = Get-MgGroup -Filter "displayName eq 'CA-Vyjimky'"
Get-MgIdentityConditionalAccessPolicy -All |
  Where-Object { $g.Id -in $_.Conditions.Users.ExcludeGroups } |
  Select-Object DisplayName, State

Get-MgGroupMember -GroupId $g.Id -All | ForEach-Object {
  Get-MgUser -UserId $_.Id `
    -Property displayName,accountEnabled,signInActivity
} | Select-Object DisplayName, AccountEnabled,
    @{n="Posledni"; e={$_.SignInActivity.LastSignInDateTime}}
```

*Členové skupiny CA-Vyjimky podle účelu účtu*




### 4.2.2 Dopad

Plošné zkoušení hesel (password spray) hledá právě účty bez druhého faktoru a jedno uhodnuté heslo otevře poštu a dokumenty bez upozornění. Účet bývalého zaměstnance je od března stále aktivní a heslo k němu zná člověk mimo organizaci.

### 4.2.3 Doporučení

- Skupinu zrušit. Nouzové účty přesunout do skupiny s možností přiřazení rolí, jejíž členství User Administrator ani Groups Administrator nezmění.
- Servisním účtům povolit přihlášení jen z adres organizace, nepoužívané zablokovat. Skenery posílat přes konektor Exchange Online ověřený IP adresou.
- Dočasné výjimky zrušit, na výměnu telefonu stačí Temporary Access Pass. Dodavatel ERP přejde na MFA, účet bývalého zaměstnance a testovací účet se zablokují.
- Upravené politiky týden provozovat v režimu report-only a vyhodnotit, koho by zablokovaly. Každá další výjimka má vlastníka, důvod a datum konce.

## 4.3 N-011 — Dvě aplikace smí číst a mazat poštu ve všech schránkách

| Vlastnost | Hodnota |
|---|---|
| Oblast | Aplikace |
| Priorita | **Vysoká** |
| Typ | Exponované ven |
| Pracnost | Střední |

### 4.3.1 Zjištěný stav

Registrace ERP-Faktury a Helpdesk-Import mají aplikační oprávnění Mail.ReadWrite k Microsoft Graph pro všechny schránky, i když každá potřebuje jen jednu. ERP-Faktury se ověřuje tajným klíčem platným dva roky, uloženým čitelně na serveru ERP. Souhlas aplikacím navíc smí udělovat každý uživatel a tři aplikace od neověřeného vydavatele tak čtou poštu.

*Ověření: aplikace s Mail.ReadWrite a nastavení souhlasu uživatelů*

```
$appId = "00000003-0000-0000-c000-000000000000"   # Microsoft Graph
$graph = Get-MgServicePrincipal -Filter "appId eq '$appId'"
$role  = $graph.AppRoles | Where-Object Value -eq "Mail.ReadWrite"
Get-MgServicePrincipalAppRoleAssignedTo -All `
    -ServicePrincipalId $graph.Id |
  Where-Object AppRoleId -eq $role.Id |
  Select-Object PrincipalDisplayName, CreatedDateTime
$p = Get-MgPolicyAuthorizationPolicy   # *-legacy = bez omezení
$p.DefaultUserRolePermissions.PermissionGrantPoliciesAssigned
```

### 4.3.2 Dopad

Kdo získá tajný klíč, přečte a smaže poštu kterékoli schránky, odkudkoli a bez přihlášení uživatele. Conditional Access pro aplikace vyžaduje licenci Workload ID Premium, kterou organizace nemá, a přihlášení aplikací nikdo nesleduje.

### 4.3.3 Doporučení

- Obě aplikace omezit na jejich schránku přes RBAC for Applications v Exchange Online a ověřit příkazem Test-ServicePrincipalAuthorization.
- Teprve potom odebrat oprávnění Mail.ReadWrite v Entra ID. Oprávnění z Entra ID a z Exchange se sčítají, bez odebrání omezení nic nezmění.
- Tajný klíč ERP-Faktury nahradit neexportovatelným certifikátem a klíč odebrat.
- Souhlas uživatelů nahradit admin consent workflow a odebrat tři aplikace od neověřeného vydavatele.

*Omezení ERP-Faktury na sdílenou schránku faktury, Exchange Online PowerShell*

```
New-ServicePrincipal -AppId $erpAppId -ObjectId $erpSpId `
    -DisplayName "ERP-Faktury"
New-ManagementScope -Name "Faktury" `
    -RecipientRestrictionFilter "Alias -eq 'faktury'"
New-ManagementRoleAssignment -App $erpSpId `
    -Role "Application Mail.ReadWrite" -CustomResourceScope "Faktury"
Test-ServicePrincipalAuthorization -Identity $erpSpId -Resource faktury
```

# 5. Roadmapa

Pořadí stojí na závislostech, ne na prioritě. Nouzové účty a upozornění na jejich přihlášení jdou před jakoukoli změnou Conditional Access, protože chyba v politice může zamknout všechny správce. Spravované zařízení se začne vyžadovat až po zašifrování zbylých 38 počítačů, jinak by je nové pravidlo zablokovalo.

*Harmonogram (týdny)*




| Krok | Obsah | Nálezy | Pracnost |
|---|---|---|---|
| 1 | Zavřít RDP a veřejný kontejner, přeposílání ven povolit jen jedné integraci | N-010, N-008 | Nízká |
| 2 | Nouzové účty s bezpečnostními klíči, export záznamů a upozornění na přihlášení nouzového účtu | N-002, N-013 | Nízká |
| 3 | Oddělené účty správců a metody odolné proti phishingu | N-001, N-005 | Střední |
| 4 | Zrušit skupinu výjimek, blokovat kód zařízení a starší ověřování, omezit aplikace na konkrétní schránky | N-003, N-004, N-011 | Vysoká |
| 5 | Zašifrovat zbylé počítače, pravidla ASR do blokování, pak vyžadovat spravované zařízení | N-007, N-006 | Vysoká |
| 6 | Sdílení a hosté, Defender for Cloud, zámky a diagnostika v Azure | N-009, N-012 | Nízká |

> Uživatelé pocítí dvě změny. Správci se budou přihlašovat metodou odolnou proti phishingu a z nespravovaných zařízení půjde k poště a souborům jen v prohlížeči bez stahování. Obě změny je potřeba ohlásit s předstihem.

# 6. Přílohy

## 6.1 Registr nálezů

| ID | Nález | Priorita | Typ | Pracnost |
|---|---|---|---|---|
| N-001 | Šest trvalých globálních správců | Kritická | Exponované ven | Střední |
| N-002 | Nikdo nehlídá nouzové účty, jeden nemá MFA | Střední | Nedoladěné | Nízká |
| N-003 | 21 účtů ve výjimce z Conditional Access | Kritická | Exponované ven | Vysoká |
| N-004 | Kód zařízení a starší ověřování neblokované | Vysoká | Exponované ven | Nízká |
| N-005 | Správci bez metody odolné proti phishingu | Vysoká | Exponované ven | Střední |
| N-006 | Přístup ze 74 nespravovaných zařízení | Vysoká | Exponované ven | Vysoká |
| N-007 | 38 počítačů bez šifrování, ASR jen v auditu | Střední | Nedoladěné | Střední |
| N-008 | Přeposílání ven povolené všem schránkám | Vysoká | Exponované ven | Nízká |
| N-009 | Odkazy bez konce platnosti, neaktivní hosté | Střední | Exponované ven | Nízká |
| N-010 | Veřejný kontejner s výkresy, otevřené RDP | Kritická | Exponované ven | Nízká |
| N-011 | Dvě aplikace s přístupem ke všem schránkám | Vysoká | Exponované ven | Střední |
| N-012 | Defender for Cloud jen základní, bez zámků | Nízká | Nedoladěné | Nízká |
| N-013 | Záznamy Entra ID se drží jen 30 dní | Střední | Nedoladěné | Nízká |

## 6.2 Politiky Conditional Access — přehled

Pět z devíti stávajících politik ke změně a tři, které chybí. Všechny stávající kromě podmínek použití pro hosty vylučují skupinu CA-Vyjimky (N-003).

| Politika | Stav | Návrh |
|---|---|---|
| MFA pro všechny uživatele | Zapnuto | Vyloučit jen nouzové účty |
| MFA pro správcovské role | Zapnuto | Ověření odolné proti phishingu (N-005) |
| Blokovat starší ověřování | Jen sledování | Zapnout po týdnu vyhodnocení (N-004) |
| MFA pro portály správy Azure | Zapnuto | Sloučit s politikou pro správce |
| Blokovat přístup mimo EU | Zapnuto | Na cesty výjimka jen z této politiky |
| Blokovat přihlášení kódem zařízení | Chybí | Založit (N-004) |
| Servisní účty jen z adres organizace | Chybí | Založit (N-003) |
| Nespravovaná zařízení jen v prohlížeči | Chybí | Založit (N-006) |