CSIRT.SK

Bezpečné nastavenie prístupu do cloudového prostredia

Odporúčanie VJ CSIRT

29.11.2023

1. Konfigurácia Multifaktorovej autentifikácie (MFA)

Použitím dodatočného spôsobu autentifikácie na vstup do cloudového prostredia je možné minimalizovať pravdepodobnosť neoprávneného prístupu. Jedným zo spôsobov dodatočnej autentifikácie je použitie **Multifaktorovej autentifikácie** (*skr. MFA*). Použitie MFA sa odporúča aj pri iných systémoch, než len v cloudovom prostredí, ak to daný systém podporuje.

1.1. Špecifikácia MFA

Multifaktorová autentifikácia požaduje od používateľa, ktorý sa snaží prihlásiť do daného prostredia, zadanie sekundárnej bezpečnostnej frázy, ktorá môže nadobudnúť viacero foriem:

- **Číselný reťazec** – Označovaný aj ako **TOTP** (*angl. Time-based One-Time Password*), kde sa zväčša jedná o 6-číselný kód, ktorý je platný iba na obmedzený čas. Po uplynutí tohto času sa generuje nový 6-číselný kód, čo efektívne limituje možnosť náhodného uhádnutia tohto číselného reťazca. Dnes existuje množstvo aplikácií, ktoré boli vytvorené za účelom generovania TOTP, medzi nich patrí napríklad Microsoft Authenticator, Google Authenticator, Authy, a veľa ďalších.
- **SMS správa** – Na telefónne číslo, ktoré je naviazané na konkrétneho používateľa, resp. na jeho konto, sa odošle SMS správa, ktorá obsahuje unikátny kód. Tento kód sa následne zadáva do systému ako sekundárna autentifikácia.
- **Emailový token** – Podobne ako pri SMS správe, aj tu sa na konkrétny používateľský email pošle unikátny kód, ktorý používateľ zadáva do systému ako sekundárnu autentifikáciu.
- **Bezpečnostné otázky** – Používateľ si počas tvorby konta vyberie niekoľko bezpečnostných otázok, ktoré mu ponúkne daný systém (väčšinou ide aspoň o 3 otázky), na ktoré by mal vedieť odpoveď iba používateľ. Po prihlásení treba na tieto otázky korektne odpovedať.

Vyššie uvedené metódy poukazujú iba na vybranú skupinu spôsobov aplikovania MFA. Vo všeobecnosti by sa však pre úspešné aplikovanie MFA mala okrem používateľského hesla využiť ešte aspoň jedna ďalšia bezpečnostná identita, menovite môže ísť o:

- **Niečo, čo viem** – Jedná sa o informáciu, ktorú pozná iba používateľ, resp. sa k nej vie dopracovať iba používateľ. Príkladom je použitie **TOTP**, bezpečnostných otázok, a podobne.
- **Niečo, čo mám** – Môže ísť o overenie pomocou druhotného fyzického zariadenia, ktoré vlastní iba konkrétny používateľ, napr. prístupová karta.
- **Niečo, čo som** – Táto identita sa odkazuje na nejakú osobnostnú vlastnosť, ktorá je príznačná pre konkrétneho používateľa. Príkladom môže byť fotografia

používateľa, alebo modernejší prístup pomocou **biometrie** (hlasová biometria, odtlačky prstov, atď.).

- **Niekde, kde som** – Druhým faktorom autentifikácie môže byť aj lokalita, na ktorej sa konkrétny používateľ nachádza. Prihlásenie do určitej platformy môže byť povolené iba z presne stanovenej geografickej polohy.

Nastavenie Multifaktorovej autentifikácie do systémov v cloudovom prostredí možno považovať za nevyhnutné, najmä pri systémoch, ktoré sú pre danú organizáciu kritické. Odporúčame aplikovať MFA primárne na administrátorské kontá, ale taktiež aj na kontá bežných používateľov, keďže aj tie môžu byť cielené potenciálnymi útočníkmi.

Za VJ CSIRT odporúčame ako minimálne opatrenie aplikovať **TOTP** na všetky kontá, ktoré by mohli predstavovať potenciálny bod prieniku do cloudového prostredia organizácie, nech už ide o administrátorské, alebo o používateľské konto. Ďalšou možnosťou je použitie **geolokácie** na povolenie prístupu na konkrétny systém iba z vybraných lokalít. Určenie povolenej lokality by malo byť čo najpresnejšie, teda môže ísť o povolenie prístupu iba z priestorov organizácie, prípadne z blízkeho okolia organizácie. Za menej bezpečnú alternatívu sa považuje aj limitovanie prístupu iba z oblasti Slovenskej republiky. Prístup do internej siete z povolenej lokality je možné regulovať aj pomocou **VPN služieb**, a to v prípade, že je povolený prístup iba z priestorov organizácie a vybraní zamestnanci potrebujú vzdialený prístup do interných systémov.

1.2. Konfigurácia MFA v prostredí Microsoft 365

Microsoft 365 poskytuje organizácii použiť tzv. **Security defaults**, ktoré implicitne vyžadujú nastavenie MFA pre všetky používateľské a administrátorské kontá. Použitie MFA sa môže viazať na akúkoľvek TOTP aplikáciu tretej strany, alebo priamo na aplikáciu Microsoft Authenticator.

Zapnutie Security defaults taktiež znamená, že od používateľov bude vyžadovaná dodatočná autentifikácia cez TOTP pri prihlásení sa do nových zariadení, alebo pri vykonávaní kritických úkonov v systéme. Administrátorské kontá sú navyše dodatočne chránené tým, že sa od nich vyžaduje zadanie TOTP pri každom prihlásení.

Ak by organizácii nevyhovovali základné nastavenia po zapnutí Security defaults, Microsoft 365 poskytuje možnosť vytvoriť si vlastné politiky prístupu a používania MFA. Označuje sa to ako **Conditional Access**. V rámci Microsoft 365 **nie je možné** používať Security defaults a Conditional Access naraz, je nutné si vybrať iba jednu z týchto dvoch metód.

Za VJ CSIRT odporúčame použitie Conditional Access, pretože je dostupná vysoká granularita nastavení pre MFA, ale aj pre mnoho ďalších bezpečnostných aspektov systému.

Viac informácií, spolu s konkrétnymi návodmi na konfiguráciu, nájdete v oficiálnej dokumentácii od Microsoft-u: https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-turn-on-mfa

2. Oddelenie administrátorských účtov od používateľských

Administrátorské kontá by mali slúžiť iba na to, čo plynie z ich názvu – administráciu. Nemali by byť používané na bežné používateľské aktivity, ako napr. používanie emailových služieb. Dôvodom je, že administrátorské kontá sú obzvlášť náchylné na útoky, keďže majú vyššie privilégiá v danom systéme. Oddelením týchto účtov od tých bežných používateľských zvyšuje úroveň bezpečnostných opatrení a pozitívne prispieva prevencii proti kybernetickým útokom.

Prístupy do administrátorských účtov by mali poznať výhradne iba **administrátori**, teda osoby, ktoré sú zodpovedné za spravovanie nejakej časti cloudového prostredia organizácie. Bežný používateľ by nemal mať žiadnu vedomosť o tom, že v systéme existuje administrátorské konto. Používateľovi stačí vedieť koho má kontaktovať, ak by potreboval služby systémového administrátora.

V rámci systému je vhodné vytvorenie aspoň jedného **globálneho administrátorského konta**, teda takého konta, z ktorého je možné spravovať všetky časti cloudového prostredia organizácie. Osoba, poverená prístupmi do globálneho administrátorského konta, by mala byť dôveryhodná a zodpovedná, keďže jej je zverené konto s vysokými systémovými privilégiami. Následne je možné vytvoriť tzv. **lokálne administrátorské kontá**, ktoré by mali prístup iba ku konkrétnemu obsahu cloudového prostredia organizácie. Lokálni administrátori väčšinou spravujú iba časť systému, napr. emailové služby, dokumentový server organizácie, a podobne. Treba dbať samozrejme na to, aby bol počet administrátorských účtov **limitovaný iba na potrebný počet**, teda nie je žiadúce udeliť administrátorský prístup priveľa používateľom. V takom prípade by sa efektivita tohto riešenia vytratila.

Pripomíname, že administrátorské kontá by mali obzvlášť **podporovať MFA**, keďže ide o kontá s vysokými privilégiami. Na administrátorské kontá, rovnako ako aj na tie používateľské, by sa mali vzťahovať **princípy RBAC a least-privilege**.

2.1. Zabezpečenie pre administrátorské kontá v prostredí Microsoft 365

Možnosti zabezpečenia administrátorských účtov, spolu s ich oddelením od tých používateľských, nájdete na oficiálnej dokumentácii od Microsoft-u: https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-protect-admin-accounts

3. Nastavenie prístupov podľa princípov RBAC a least-privilege

Princípy **Role-based Access Control** (*skr. RBAC*) a **least-privilege** predstavujú také opatrenie, kde sú konkrétnemu používateľovi pridelené privilégiá podľa roly, ktorá mu v organizácii prislúcha, a ktoré mu umožňuje v systéme vykonávať iba aktivity potrebné na plnenie jeho pracovnej činnosti.

3.1. Špecifikácia RBAC

Aplikovanie RBAC do cloudového prostredia znamená vytvorenie niekoľkých požadovaných rolí. Tieto roly môžu byť rôzne, niektoré môžu používateľovi povoliť iba čítanie dát zo systému, niektoré aj zápis do systému, prípadne vykonávať zmeny uložených dát v systéme, alebo ich vymazávať. **Granularita rolí** by mala byť čo **najvyššia**, aby sa konkrétnemu používateľovi dali prideliť iba tie role, ktoré skutočne potrebuje na vykonanie svojej pracovnej činnosti. Zároveň by sa roly mali dať aj kombinovať, keďže jeden používateľ môže potrebovať prístupy do viacerých častí cloudového prostredia. Typicky teda vieme rozlíšiť nasledujúce povolenia pre dané roly:

- **Čítanie** (*angl. Read*) – Používateľ vie z vybranej časti systému čítať dáta, nevie ich nijako upravovať, ani vytvárať.
- **Zápis** (*angl. Write*) – Používateľ vie vo vybranej časti systému vytvárať dáta. Udelenie týchto povolení sa často kombinuje s Read povoleniami.
- **Úprava** (*angl. Edit*) – Používateľ vie vo vybranej časti systému upravovať už existujúce dáta.
- **Vymazávanie** (*angl. Delete*) – Používateľ vie vo vybranej časti systému vymazávať existujúce dáta.

Rola následne okrem vyššie uvedených povolení presnejšie určuje časť systému, na ktorú sa povolenie vzťahuje. Príkladom môžu byť fiktívne roly „*DB_access_Read*“ a „*DB_access_Write*“. Používateľ A s pridelenou rolou „*DB_access_Read*“ môže z vybranej databázy dáta iba čítať, zatiaľ čo používateľ B s pridelenými oboma rolami „*DB_access_Read*“ a „*DB_access_Write*“ môže z vybranej databázy dáta čítať a môže ich tam aj vytvárať. Ani jeden z používateľov však dáta v databáze nemôže upravovať, ani vymazávať, keďže im na to nebola udelená rola.

Organizácia si tieto role môže upraviť podľa svojich potrieb. Nie je limitovaná iba na uvedené 4 povolenia (Read, Write, Edit, Delete), môže si vytvoriť aj vlastné povolenia, ak je to nutné.

3.2. Špecifikácia least-privilege prístupov

Princípy least-privilege oprávňujú používateľov pristupovať v cloudovom prostredí iba tam, kde to potrebujú, resp. kde musia mať prístupy na splnenie svojej pracovnej činnosti. Príkladom môže byť, že zamestnancovi na oddelení zákazníckej podpory by sme neudelili prístup do interných systémov Personálneho oddelenia, keďže si to nevyžaduje jeho pracovná náplň. Navyše by sme takto zbytočne vytvorili ďalší potenciálny bod prieniku do interných systémov organizácie.

Z toho dôvodu by mala byť granularita RBAC vysoká, aby sme vedeli používateľom prideliť len minimálne privilégiá. Princípy RBAC a least-privilege v tomto úzko spolupracujú, aby sme predišli situácii typu „všetci majú prístup všade“, čo by znamenalo, že úspešný útok na jedno používateľské konto môže viesť k rozsiahlemu útoku na celú organizáciu.

3.3. Konfigurácia RBAC a least-privilege v prostredí Microsoft 365

V rámci Microsoft 365 už vybrané roly existujú. Tieto roly je možné využiť pri konfigurácii RBAC v rámci organizácie. Oficiálna dokumentácia od Microsoft-u obsahuje kapitolu, kde sú stanovené minimálne roly pre konkrétne úlohy v prostredí Microsoft 365, prípadne v prostredí **Microsoft Azure**: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task

Pre rozsiahlejšie informácie o možnostiach aplikovania RBAC odporúčame navštíviť dokumentáciu **Microsoft Entra**, kde nájdete množstvo návodov na implementovanie RBAC a least-privilege princípov do cloudového prostredia organizácie: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/

4. Princípy zero-trust infraštruktúry

Princípy RBAC a least-privilege sa často spájajú s konceptom **zero-trust**, ktorý je vhodné implementovať na zabezpečenie cloudovej infraštruktúry zvnútra organizácie, nie iba z externého prostredia. Jedná sa o bezpečnostný koncept, kde sa pre každá sieťová lokalita implicitne považuje za nedôveryhodnú. Následne je vybraný a manuálne nastavený iba užší okruh sieťových lokalít, ktorý je možné kontaktovať aj z cloudového, alebo interného prostredia organizácie.

Prístup do Internetu je preto v zero-trust infraštruktúre všeobecne obmedzený iba na vyhradené lokality na základe viacerých faktorov, ako napr. pridelené role, oprávnenia používateľa v rámci infraštruktúry, alebo špecifickejšie aspekty ako bezpečnostná história danej lokality. Konkrétnou implementáciou vybraných zero-trust konceptov je napríklad nasadenie a používanie **štandardu 802.1X**.

Z praktického hľadiska si zero-trust infraštruktúru vieme predstaviť ako sieť, ktorá je skrytá za firewallom, pričom firewall implicitne blokuje všetku premávku smerujúcu z internej siete do Internetu. Sieťový administrátor následne povolí prechod cez firewall do Internetu iba tým doménam, ktoré sú nevyhnutné pre vykonávanie pracovnej činnosti zamestnancov. Zvyšok je naďalej blokovaný a skupina povolených domén sa mení iba po schválení a manuálnom nastavení firewallu sieťovým administrátorom. Rovnakým spôsobom sa potom zabezpečí prístup opačným smerom, teda smerom z Internetu do internej siete. Samozrejme, jedná sa o triviálny príklad, avšak pomáha nám lepšie si vizualizovať zero-trust princípy.

Zero-trust koncept je taktiež založený na **správe identít**, ktoré v internej sieti máme. Prístup by preto mali dostať iba autentifikovaní používatelia, napr. cez vyššie spomenutý štandard 802.1X. Jedným z vhodných spôsobov, ako spravovať prístupy v organizácii pre prostredie Microsoft 365 je použitie **Active Directory**, alebo **Microsoft Intune**. Viac sa o týchto možnostiach môžete dočítať na oficiálnej dokumentácií od Microsoft-u:

- **Active Directory:** https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration
- **Microsoft Intune:** https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Implementáciou zero-trust princípov vieme lepšie kontrolovať a monitorovať prístup do cloudového prostredia. Treba však dbať na to, aby boli tieto princípy korektne nastavené a najmä dodržiavané, aby si organizácia namiesto bezpečnostného opatrenia nevytvorila bezpečnostné riziko.

5. Odporúčaná politika hesiel

Nastavenie bezpečných hesiel pre všetkých používateľov si vyžaduje vopred stanovenú politiku, ktorá jasne určuje rôzne aspekty hesiel. Vytvorená politika by mala jasne určovať pre koho je platná, avšak odporúčame politiku hesiel aplikovať na všetkých zamestnancov danej organizácie.

5.1. Špecifikácia všeobecnej politiky hesiel

Politika hesiel môže zahŕňať niekoľko bodov, ktoré by používatelia mali dodržiavať pri tvorbe nových hesiel, alebo pri ich obnovovaní. Menovite ide o nasledujúce body:

- **Povolená konfigurácia:**
  - Dĺžka hesla by mala predstavovať **minimálne 12 znakov**
  - Používať kombináciu alfanumerických znakov a špeciálnych znakov
  - Používať kombináciu veľkých a malých písmen
  - Uprednostniť **bezpečnostnú frázu**, pred klasickým heslom
  - Používať **multifaktorovú autentifikáciu** (*skr. MFA*)
  - **Pravidelne meniť používateľské heslo** po určitej dobe (napr. každých 6 mesiacov)
- **Nepovolená konfigurácia:**
  - Nepoužívať jednoslovné heslá
  - Nepoužívať dobre známe, alebo ľahko uhádnuteľné heslá
  - Nepovoliť opakované použitie rovnakých hesiel pri potrebe jeho zmeny
  - Nepovoliť použitie rovnakého hesla na viacero webových lokalít
  - Nepoužívať osobné údaje ako súčasť hesiel

Uvedené body je vhodné aplikovať na bežné kontá, ale najmä na administrátorské kontá, alebo iné kontá, ktoré majú zvýšené privilégiá. Táto politika by mala byť aplikovaná už pri tvorbe hesiel, či už pre nových, alebo dlhodobých zamestnancov danej organizácie. Kontrola sily hesiel by mala prebiehať **automatizovane**, teda vyššie uvedené podmienky by mali byť kontrolované počítačom už počas nastavovania hesla. V opačnom prípade musí organizácia pristúpiť k inej forme kontroly, za účelom vynucovania stanovenej politiky hesiel.

5.2. Konfigurácia politiky hesiel v prostredí Microsoft 365

Microsoft 365 ponúka viacero možností ako splniť uvedené body v špecifikácii politiky hesiel. Za VJ CSIRT najviac odporúčame zavedenie **MFA**, ale samozrejme netreba zabúdať ani na ostatné aspekty bezpečných hesiel.

Politiku hesiel pre prostredie Microsoft 365 je možné nastaviť cez **Microsoft Entra** podľa oficiálnej dokumentácie od Microsoft-u: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy

Dodatočné odporúčania pre bezpečné heslá nájdete na Microsoft 365 dokumentácii na nasledujúcom odkaze: https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations

6. Zvyšovanie povedomia zamestnancov o kybernetickej bezpečnosti

Nastavenie určitých bezpečnostných opatrení na systémoch v cloudovom prostredí predstavuje iba časť z celého procesu ochrany proti kybernetickým útokom. Treba dbať na to, že kritickým bodov sú často zamestnanci organizácie, ktorí nie sú dostatočne vzdelaní v oblasti kybernetickej bezpečnosti na používateľskej úrovni. Veľa zamestnancov má problém rozlíšiť spam od validnej správy, čo môže viesť k prieniku do systémov organizácie (aj keď je to zo strany zamestnanca neúmyselné). Zvyšovanie povedomia vlastných zamestnancov patrí k jednému z najpodstatnejších odporúčaní, ktoré ako Vládna jednotka CSIRT dávame organizáciám.

Dnes existuje množstvo školení a workshopov, ktoré pomáhajú používateľom rozoznávať pokusy o útok od bezpečných aktivít vo virtuálnom prostredí. Veľa organizácií si tieto školenia rieši aj interne. Vládna jednotka CSIRT taktiež poskytuje podobné školenia, hlavne za účelom predídenia kybernetickým útokom a zabráneniu chybného vyhodnocovania škodlivej aktivity na Internete od zamestnancov danej organizácie. Udržiavanie kybernetickej bezpečnosti je cyklická záležitosť, teda treba ju pravidelne rozvíjať a držať sa aktuálnych trendov. Školenie vlastných zamestnancov je neoddeliteľnou súčasťou tohto cyklu, preto naň netreba zabúdať.

7. Dodatočné zdroje

Za účelom získania ďalších informácií o princípoch, uvedených v tomto dokumente, sem pridávame ďalšie zdroje, ktoré opisujú aplikáciu týchto princípov aj do iných platforiem, prípadne rozširujú implementáciu do platformy Microsoft 365 a jej súčastí.

Amazon AWS

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/access.html

https://docs.aws.amazon.com/IAM/latest/UserGuide/security.html

Microsoft 365

https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-security-overview?view=o365-worldwide

Microsoft Azure

https://learn.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

Google Cloud

https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

Zero-trust princípy pre Microsoft 365

https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

Prehľad ISO štandardov

https://www.csirt.gov.sk/prehlad-standardov-iso-iec-27000.htm