Prehľad bezpečnosti — **monokaido.com**

> Verejný dokument popisujúci bezpečnostné princípy, opatrenia a osvedčené postupy zavedené v platforme Monokaido. Cieľom je transparentne priblížiť, ako chránime dáta našich zákazníkov a ich koncových používateľov.

Platforma	Monokaido — multi-tenant SaaS PIM (Product Information Management) s e-commerce funkciami
Charakter dokumentu	Verejný prehľad bezpečnosti (Security & Trust Overview)
Posledná aktualizácia	2026-06-27

---

1. Úvod

Bezpečnosť je v platforme Monokaido navrhnutá ako **súčasť architektúry od základu**, nie ako dodatočná vrstva. Pri vývoji uplatňujeme tri hlavné princípy:

- **Security by design** — bezpečnostné kontroly sú zabudované priamo do návrhu funkcií, nie pridávané dodatočne.
- **Defense in depth (obrana do hĺbky)** — kľúčové oblasti sú chránené viacerými nezávislými vrstvami, takže zlyhanie jednej vrstvy ešte neznamená kompromitáciu.
- **Least privilege (princíp najmenších oprávnení)** — každá súčasť systému aj každý používateľ majú prístup len k tomu, čo nevyhnutne potrebujú.

Tento dokument zhŕňa konkrétne opatrenia, ktoré tieto princípy napĺňajú.

2. Šifrovanie a ochrana dát

Dáta pri prenose (in transit)

- Všetka komunikácia s platformou prebieha výhradne cez **šifrované spojenie HTTPS (TLS)**.
- Podporujeme len moderné, bezpečné verzie protokolu **TLS 1.2 a TLS 1.3**; staršie, zraniteľné verzie sú zakázané.
- Nešifrovaný prístup je automaticky presmerovaný na zabezpečené spojenie.
- Nasadené je **HSTS** (HTTP Strict Transport Security), ktoré prehliadačom prikazuje komunikovať s platformou výhradne cez HTTPS.

Dáta v pokoji (at rest)

- Citlivé prístupové údaje (napr. integračné prihlasovacie údaje k systémom dodávateľov) sú v databáze **šifrované moderným autentifikovaným šifrovaním AES-256-GCM**.
- Šifrovanie využíva výlučne overené, štandardné kryptografické knižnice — **nepoužívame vlastné („domácke") kryptografické riešenia**.
- Každá zašifrovaná hodnota má vlastný náhodný inicializačný vektor a kryptografický autentifikačný štítok, ktorý sa pri dešifrovaní overuje (ochrana proti neoprávnenej úprave dát).
- Sila a integrita šifrovacieho kľúča sa **overuje už pri štarte systému** — pri nesprávnej konfigurácii sa služba nespustí.

---

3. Autentifikácia a správa identít

- **Heslá nikdy neukladáme v čitateľnej podobe.** Ukladajú sa výhradne ako jednosmerný kryptografický odtlačok pomocou algoritmu **bcrypt** s primeraným výpočtovým nákladom.

- **Ochrana proti útokom hrubou silou (brute-force):** po opakovaných neúspešných pokusoch o prihlásenie sa účet dočasne uzamkne, pričom dĺžka uzamknutia **postupne narastá** pri ďalších pokusoch.
- **Rate limiting (obmedzenie frekvencie):** prihlasovanie, registrácia, obnova hesla a ďalšie citlivé operácie majú prísne limity počtu požiadaviek, a to na viacerých úrovniach infraštruktúry súčasne.
- **Odolnosť proti enumerácii používateľov:** prihlasovací proces je navrhnutý tak, aby útočník nedokázal podľa odpovede ani podľa času spracovania rozlíšiť neexistujúci účet od nesprávneho hesla.
- **Bezpečná obnova hesla:** tokeny na obnovu hesla majú vysokú entropiu, ukladajú sa len v podobe odtlačku, sú **jednorazové** a majú **krátku časovú platnosť**. Odkazy na obnovu sú overované voči dôveryhodným doménam zákazníka.

---

4. Správa relácií (sessions)

- Prihlasovacie tokeny administrátorskej časti sú uložené v **HttpOnly cookies** — nie sú prístupné z JavaScriptu, čo výrazne znižuje riziko ich zneužitia.
- Cookies sú označené atribútmi **Secure** (prenášané len cez HTTPS) a **SameSite=Strict**, čo poskytuje silnú ochranu proti útokom typu CSRF (Cross-Site Request Forgery).
- Prístupové a obnovovacie tokeny sú od seba kryptograficky oddelené a majú **rozdielnu, primerane krátku životnosť**.
- Oprávnenia používateľa sa **overujú pri každej požiadavke** voči aktuálnemu stavu v databáze — deaktivovaný alebo uzamknutý účet stráca prístup okamžite.

---

5. Riadenie prístupu a izolácia zákazníkov (multi-tenancy)

Monokaido je multi-tenant platforma — viacero zákazníkov (firiem) zdieľa tú istú aplikáciu, no ich dáta sú **dôsledne oddelené**.

- **Oddelenie dát na úrovni aplikácie:** každý prístup k dátam je viazaný na konkrétneho zákazníka, takže používateľ vidí výhradne dáta vlastnej organizácie.
- **Row-Level Security (RLS):** databáza je navrhnutá s politikami izolácie na úrovni jednotlivých riadkov ako **ďalšia obranná vrstva** nad aplikačným oddelením dát. Tieto politiky sú navrhnuté podľa princípu **fail-closed** — pri chýbajúcom kontexte nevrátia žiadne dáta (nikdy nie všetky).
- **Riadenie prístupu na základe rolí (RBAC):** používatelia majú priradené role s rôznou úrovňou oprávnení; citlivé operácie sú dostupné len rolám, ktoré na ne majú právo, pričom rola sa overuje voči databáze.
- **Bezpečné prepínanie medzi organizáciami:** používateľ sa môže prepnúť len do organizácie, ktorej je preukázateľne aktívnym členom; rola sa odvodzuje zo servera, nie z údajov poslaných klientom.
- **Ochrana pred neoprávneným priradením oprávnení:** používateľ si nemôže sám zvýšiť rolu ani priradiť prístup, ktorý mu neprislúcha — všetky takéto operácie sú riadené administrátorom a overované na strane servera.

---

6. Ochrana pred bežnými webovými útokmi (OWASP)

Platforma je systematicky chránená proti najbežnejším triedam zraniteľností podľa rebríčka **OWASP Top 10**.

Ochrana proti SQL injection

- Všetky databázové dotazy používajú **parametrizované dotazy** — používateľský vstup sa nikdy nespája priamo do textu SQL príkazu.
- Aj prvky, ktoré sa nedajú parametrizovať (napríklad názvy stĺpcov pri triedení), sú obmedzené na **pevný zoznam povolených hodnôt (allow-list)**.

Ochrana proti Cross-Site Scripting (XSS)

- Všetok obsah generovaný používateľmi alebo externými zdrojmi, ktorý sa zobrazuje ako HTML, prechádza **centralizovanou sanitizáciou** cez overenú knižnicu (DOMPurify) s prísnym zoznamom povolených značiek a atribútov.
- Nasadené sú bezpečnostné HTTP hlavičky vrátane **Content Security Policy (CSP)**, **X-Content-Type-Options** a ďalších, ktoré obmedzujú možnosti zneužitia v prehliadači.

Ochrana proti CSRF (Cross-Site Request Forgery)

- Architektúra autentifikácie je navrhnutá tak, aby požiadavky nebolo možné sfalšovať z cudzej stránky (kombinácia `SameSite=Strict` cookies a autentifikácie cez hlavičky).

Ochrana proti SSRF (Server-Side Request Forgery)

- Pri spracovaní externých zdrojov (napr. dodávateľské feedy, externé obrázky) platforma **validuje cieľové adresy** a blokuje pokusy o prístup do internej siete či k metadátovým službám.
- Súčasťou ochrany je **overovanie skutočne preloženej IP adresy**, kontrola pri každom presmerovaní a obmedzenie na bezpečné protokoly.

Bezpečné spracovanie vstupov

- Všetky vstupné dáta sú **striktne validované** podľa očakávanej štruktúry; neznáme alebo nadbytočné polia sú automaticky odmietnuté (ochrana proti tzv. mass-assignment).
- Operácie so súbormi sú chránené proti útokom typu **path traversal** (pokus o prístup mimo povoleného priestoru).

---

7. Bezpečnosť platieb a e-commerce

- **Citlivé platobné údaje (čísla kariet) nikdy neukladáme** v našich systémoch. Platby spracúvajú renomovaní, certifikovaní platobní poskytovatelia (v súlade s **PCI DSS**).

- **Ceny a sumy objednávok sa vždy prepočítavajú na strane servera** z dôveryhodných údajov v databáze — klient nikdy neurčuje výslednú cenu. Tým je vylúčená manipulácia s cenami či súčtami.
- **Platobné notifikácie (webhooky) sa kryptograficky overujú** ešte pred spracovaním. Objednávka sa označí ako uhradená až po overení od platobnej brány, nikdy nie na základe údajov z prehliadača zákazníka.
- Implementovaná je **ochrana proti duplicitnému spracovaniu a opakovaniu (replay)** platobných notifikácií.
- Operácie s citlivým dopadom (sklad, zľavy, vernostné body, objednávky) sú chránené **databázovým zamykaním**, ktoré zabraňuje súbežným nekonzistentným zmenám (napr. dvojitému uplatneniu jednorazovej zľavy alebo predaju nedostupného tovaru).
- Veľkoobchodné a nákladové údaje (napr. nákupné ceny) sú **nikdy nevystavené** vo verejných rozhraniach — verejné odpovede obsahujú výlučne explicitne povolené polia.

---

8. Infraštruktúra a sieťová bezpečnosť

- Platforma beží v **izolovaných kontajneroch**, ktoré bežia pod **neprivilegovanými používateľmi** (nie ako root).
- **Dátové úložiská a interné služby nie sú vystavené do verejného internetu** — sú dostupné len v rámci internej, oddelenej siete aplikácie.
- Verejný prístup je sústredený cez **jediný vstupný bod** (reverzná proxy), ktorý zabezpečuje šifrovanie, bezpečnostné hlavičky a obmedzovanie frekvencie požiadaviek.
- Chybové stavy sú spracované tak, aby používateľovi **neunikli interné technické detaily** (napríklad výpisy chýb či detaily databázy).

---

9. Správa tajomstiev (secrets)

- Prístupové údaje, kľúče a iné tajomstvá **nie sú nikdy súčasťou zdrojového kódu** ani verzovacieho systému.

- Konfiguračné tajomstvá sú spravované cez oddelené, chránené prostredie; zálohy citlivej konfigurácie sú **šifrované**.
- Integračné prihlasovacie údaje zákazníkov sú v databáze uchovávané výhradne v **zašifrovanej podobe**.

---

10. Bezpečný vývoj softvéru (Secure SDLC)

Bezpečnosť je integrovaná aj do samotného procesu vývoja:

- **Povinné testy pre každú zmenu** — každá úprava kódu musí byť pokrytá automatizovanými testami (opravy chýb regresnými testami, nové funkcie unit a integračnými testami).
- **Automatizovaná kontrola pred publikovaním** — zmeny musia prejsť statickou analýzou, typovou kontrolou a testami; pokým nie sú „zelené", nedostanú sa do hlavnej vetvy.
- **Povinný code review** — žiadna zmena sa nezlúči bez kontroly, vrátane automatizovaného bezpečnostného posúdenia zmien.
- **Princíp „nič sa nepublikuje s červenými testami"** — kvalita a bezpečnosť majú prednosť pred rýchlosťou.

---

11. Logovanie a súkromie

- V prevádzkových záznamoch (logoch) **nikdy neukladáme heslá, tokeny ani dešifrované tajomstvá**.
- Záznamy sú navrhnuté tak, aby umožnili diagnostiku a audit bez vystavenia citlivých údajov.
- K dátam pristupujeme v súlade s princípom najmenších oprávnení a s ohľadom na súkromie koncových používateľov.

12. Zhrnutie

Platforma Monokaido uplatňuje viacvrstvový, premyslený prístup k bezpečnosti, ktorý pokrýva celý životný cyklus dát aj vývoja:

Oblasť	**Kľúčové opatrenia**
Šifrovanie	TLS 1.2/1.3 pri prenose, AES-256-GCM pri uchovaní citlivých údajov
Autentifikácia	bcrypt, account lockout, rate limiting, odolnosť proti enumerácii
Relácie	HttpOnly + Secure + SameSite cookies, oddelené tokeny, overovanie pri každej požiadavke
Izolácia zákazníkov	Dôsledné oddelenie dát + Row-Level Security ako obrana do hĺbky
Riadenie prístupu	Role-based access control overovaný na strane servera
Ochrana proti útokom	Parametrizované dotazy, sanitizácia výstupu, CSP, ochrana proti SSRF/CSRF
Platby	Žiadne ukladanie kariet, server-side ceny, overené webhooky
Infraštruktúra	Izolované neprivilegované kontajnery, úložiská mimo internetu, HTTPS-only
Vývoj	Povinné testy, automatizované brány kvality, povinný code review

Bezpečnosť vnímame ako **kontinuálny proces**, nie ako jednorazový stav. Naše opatrenia priebežne preverujeme, vyhodnocujeme a posilňujeme tak, aby zodpovedali aktuálnym hrozbám a osvedčeným postupom v odvetví.

Mgr. Ivan Kopčík

