

Shopify a bezpečnost v cloudu

Bezpečnost v modelu SaaS (Software as a Service) funguje na principu **sdílené odpovědnosti**. Zatímco Shopify odpovídá za bezpečnost „cloudu“ (hardware, síť, aplikace), obchodník odpovídá za bezpečnost „v cloudu“ (správa hesel, oprávnění zaměstnanců, výběr aplikací).

1. Certifikace a standardy

Shopify splňuje nejprísnejší globální standardy, které jsou automaticky aplikovány na každý e-shop na platformě:

- **PCI DSS Level 1:** Jak bylo rozebráno v článku [PCI DSS](#), Shopify splňuje nejvyšší úroveň zabezpečení pro nakládání s platebními kartami.
- **SOC 2 Type II:** Nezávislý audit potvrzuje, že systémy Shopify jsou navrženy tak, aby chránily data zákazníků a zajistily dostupnost služeb.
- **GDPR a soukromí:** Shopify poskytuje nástroje pro splnění evropských předpisů na ochranu osobních údajů, včetně šifrování dat a možnosti jejich výmazu.

2. Vrstvy zabezpečení infrastruktury

Shopify využívá vícevrstvou obranu k eliminaci rizik:

- **Ochrana proti DDoS:** Integrovaná ochrana (často ve spolupráci s Cloudflare) filtruje útoky, které se snaží zahltnit server a odstavit e-shop z provozu.
- **TLS (HTTPS) certifikáty:** Každý e-shop na Shopify má automaticky generovaný SSL/TLS certifikát. Veškerá komunikace mezi zákazníkem a serverem je šifrována.
- **Bounty programy:** Shopify platí etickým hackerům (Bug Bounty), aby v jejich systému hledali zranitelnosti dříve, než je zneužijí útočníci.

[Image showing Layers of Shopify Security: Physical (Data centers), Network (DDoS protection), Application (Patching), and Merchant (2FA)]

3. Bezpečnost pro obchodníka (User Side)

I když je jádro systému bezpečné, nejslabším článkem zůstává člověk. Shopify nabízí nástroje k eliminaci těchto rizik:

- **Dvoufázové ověření (2FA):** Povinné nebo doporučené přihlašování pomocí SMS, e-mailu nebo autentizační aplikace.
- **Role a oprávnění:** Možnost vytvořit účty pro zaměstnance s omezeným přístupem (např.

- skladník vidí jen objednávky, ale nemůže měnit bankovní údaje).
- **Analýza rizik objednávek:** Integrovaný algoritmus strojového učení ([Machine Learning](#)) analyzuje každou objednávku a upozorňuje na potenciální podvody (Fraud Analysis).

4. Bezpečnost aplikací třetích stran

Aplikace z App Store mohou představovat riziko, proto Shopify zavedlo přísná pravidla:

- **API Scopes:** Aplikace musí při instalaci přesně definovat, k jakým datům potřebuje přístup.
- **Ověřování aplikací:** Každá aplikace prochází před schválením do App Store revizí kódu a bezpečnostních procesů.

5. Srovnání bezpečnosti: SaaS vs. Open-Source

Riziko	Shopify (SaaS)	Open-Source (např. Magento)
Aktualizace (Patching)	Provádí Shopify automaticky na pozadí.	Musí provádět správce (často se zapomíná).
SQL Injection	Ošetřeno v rámci platformy.	Závisí na kvalitě napsaného kódu a pluginů.
Únik dat karet	Skoro nemožné (data nejdou přes váš server).	Vysoké riziko při špatné konfiguraci serveru.

Související články:

- [Standardy platebních karet](#)
- [Obecné zabezpečení webu](#)
- [Shopify jako SaaS model](#)

Tagy: *it security shopify cloud compliance ddos gdpr encryption*

From:
<https://www.serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:
https://www.serviceit.cz/doku.php?id=it:sw:shopify_saas

Last update: **2026/01/02 20:08**

