



SIGURNOST PODATAKA

Alpina management d.o.o. ulaže razumne tehničke I organizacijske mjere radi zaštite vaših podataka.

SIGURNOST INTERNETSKJE STRANICE

Radi sigurnosti same internetske stranice alpinamanagement.Eu, kao I vaših osobnih podataka koje možete unijeti putem kanala komunikacije, uveli smo više sustava sigurnosti koje možete pronaći niže:

- SSL/TLS enkripcija - TLS_AES_256_GCM_SHA384, 256-bitni ključevi, TLS 1.3
- zaštićeni poslužitelji I redoviti backup
- ograničen pristup samo ovlaštenim osobama
- redovite revizije sigurnosti.

Niže se nalaze detalji SSL/TLS enkripcije koju koristimo:

- TLS_AES_256_GCM_SHA384 - iznimno siguran kriptografski paket (engl. Cipher suite) koji se koristi u sigurnosnim protokolima TLS 1.2 I TLS 1.3 za uspostavu šifrirane I povjerljive komunikacije između klijenta (npr. internetskog preglednika) i poslužitelja
- 256-bitni ključevi - iznimno dugačak niz jedinica I nula (duljine 32 bajta) koji se u kriptografiji koristi za zaključavanje I otključavanje podataka. Predstavlja zlatni standard za zaštitu informacija jer nudi velik broj mogućih kombinacija — broj s čak 77 znamenki, što ga čini praktički nemogućim za probijanje čak I najsnažnijim računalima
- TLS 1.3 - najnovija I najsigurnija verzija protokola transport layer security (TLS). On osigurava privatnost I cjelovitost podataka prilikom komunikacije na internetu (štiti od prisluškivanja I man-in-the-middle napada) te predstavlja tehnologiju koja se krije iza HTTPS lokota u vašem internetskom pregledniku.

Dodatno, koristimo cloudflare-ove usluge:

- AI labyrinth
- Bot fight mode
- Browser integrity check
- Cloudflare managed ruleset
- Continuous script monitoring
- Email address obfuscation
- Hotlink protection
- HTTP DDoS attack protection
- Leaked credentials detection
- Network-layer DDoS attack protection
- Replace insecure JavaScript libraries
- Schema validation
- SSL/TLS DDoS attack protection
- Web asset discovery.

Obzirom na visok stupanj sigurnosti same stranice, na neovisnom testu tvrtke ImmuniWeb dodijeljena nam je najviša razina sigurnosti ("A").



SIGURNOST KOMUNIKACIJE

Uzimajući u obzir praktičnost i sigurnost, niže vam dostavljamo popis naših platformi za kontakt i njihovu zaštitu:

- Gmail - Transport Layer Security (TLS)
- WhatsApp - E2E enkripcija
- Facebook - E2E enkripcija
- Kontakt putem forme - SSL/TLS enkripcija + Transport Layer Security (TLS).

Popis šifriranja/enkripcija:

- Transport Layer Security (TLS) - standardno šifriranje e-mail poruka.
- E2E enkripcija - metoda sigurne komunikacije kod koje se podaci šifriraju na uređaju pošiljatelja i dešifriraju isključivo na uređaju primatelja. Nitko između - ni pružatelj usluge, ni telekom operater, ni hakeri - ne može presresti ili pročitati sadržaj poruke.
- SSL/TLS enkripcija - kriptografski protokol koji stvara siguran, šifrirani kanal između poslužitelja i klijenta (NPR. Web preglednika). Sprječava neovlašteno presretanje i krađu osjetljivih podataka osiguravajući privatnost, cjelovitost i autentičnost informacija.

NAPOMENA

Internetske tehnologije nisu potpuno sigurne, a prijenos podataka može uključivati rizike.

Šifriranje otežava neovlaštenim osobama pregledavanje informacija koje putuju između računala.

Stoga je mala vjerojatnost da je netko u vašoj sesiji pročitao ovu stranicu dok je putovala mrežom.