Na koji način štitite moju WordPress instalaciju od napada?

Last updated 5. 11. 2020

O zaštiti Vaše WordPress Hosting usluge od različitih vrsta napada se staraju naši mnogobrojni servisi koji se nalaze na nivou servera. Ovi servisi se automatski aktiviraju kada zakupite uslugu i vrše konstantan nadzor i uključuju svakodnevno skeniranje sadržaja.

Serverski firewall

Firewall koji je instaliran na serverima koji su zaduženi za hosting WordPress korisnika konstantno nadgleda sav nadolazeći i odlazeći saobraćaj. Pored nadgledanja saobraćaja, posebni servisi su zaduženi i za nadgledanje pojedinačnih procesa na serveru kako bi se sprečila zloupotreba. U slučaju bilo kakvih malicioznih radnji, firewall će izvršiti privremenu ili permanentu blokadu IP adrese.

ModSecurity

ModSecurity spada u red Web Application Firewall servisa čiji je zadatak da motre i procesiraju sav HTTP saobraćaj i upoređuju svaki zahtev sa nizom predefinisanih bezbednosnih pravila. Ukoliko neki zahtev aktivira postojeće pravilo, korisnik biva momentalno blokiran od strane servera.

Na ovaj način se štite WordPress instalacije od OWASP 10 sigurnosnih propusta ali i od poznatih sigurnosnih propusta u instaliranim temama i WordPress dodacima.

Bruteforce zaštita

Sledeći u nizu odbrambenih mehanizama je servis koji isključivo nadgleda WordPress login formu (wp-login.php). Nakon 5 neuspelih pokušaja, svaki sledeći pokušaj će biti dodatno usporen od strane servera ili će od korisnika biti zahtevano da dokaže da nije bot kroz reCAPTCHA validaciju.

Na ovaj način je svaki login koji se bazira na internom WordPress mehanizmu zaštićen od bruteforce napada.

Security Report

Iako naša WordPress Hosting usluga nudi veliki broj mehanizama za uvećavanje bezbednosti, oni nisu svemogući i ubacivanje malicioznog koda je svakako moguće. To se najčešće dešava zbog neadekvatnog održavanja WordPress instalacija i instaliranih dodataka i tema.

Međutim, tu na snagu stupa Security Report – poseban servis koji svakoga dana skenira sve fajlove u okviru vašeg naloga u potrazi za malicioznim kodom. Rezultat tog skeniranja je izveštaj koji sadrži spisak potencijalnih fajlova koji mogu predstavljati problem, ali i spisak svih dodataka za koje postoji ažuriranje. Ovaj izveštaj se automatski prosleđuje svakom korisniku WordPress Hosting usluge na email.

Na taj način želimo da i korisnici budu svesni da je odgovarajuća akcija sa njihove strane potrebna kako bi njihovi WordPress sajtovi bili bezbedni.