

Izveštaj o stanju servera kancelarko.rs sa stanovišta sigurnosti podataka i pristupa

Napomena: *Iz razloga sigurnosti u izveštaju se neće imenovati instalirani softver već samo njegova namena.*

Server je zaštićen najsavremenijim hardverskim i softverskim rešenjima sa posebnim osvrtom na sledeće slabosti koji su uobičajeni za njegovu namenu (web server):

- Sertifikat za enkripciju i sigurnosnu indetifikaciju servera (*HTTPS*) – verzija *TLSv1.2*.
- Softver za zaštitu protiv *Brute Force* i *DDoS* napada.
- Softver za zaštitu i čuvanja privatnosti svih javni i privatnih ključeva za *SSH* kontrolu.
- Softver za detaljnu kontrolu pristupa osetljivim servisima sa dvostrukom autentifikacijom ukoliko IP adresa administratora nije na listi odobrenih. Ručno blokiranje celih blokova IP adresa kao i čitavih zemalja (trenutno blokirane sve zemlje osim *Serbia RS*).
- Softver za menadžment i upravljanje pravilima ponašanja servera u određenim siutacijama (*Application Policies*). U pitanju je sofisticirani softver koji kanališe ponašanje javno dostupnih aplikacija na jasno uređeni način. Ovim se sprečava svaka zlonamerna upotreba softvera od strane neautorizovanih korisnika.
- Softver za menadžment i upravljanje pravilima sigurnosnih podešavanja servera (*Security Policies*)
- Sofver za zaštitu protiv *Shell Fork Bomb* napada.
- Softver za rano otkrivanje potencijalnih slabosti servera sa sistemom obaveštavanja administratora.
- Antivirusni softver.
- Zbog bezbednosti servera, aplikacija ne dozvoljava čuvanje fajlova sa ekstenzijama koje mogu kompromitovati server već samo fajlove čija ekstenzija pripada jasno definisanom skupu dozvoljenih.
- Rigorozan firewall filter koji propušta samo komunikaciju po jasno definisanim portovima.
- Konfiguracija složenosti lozinki korisnika sa *SSH* pristupom (zahtevnost upotrebe izuzetno složenih lozinki za korisnike sa *SSH* pristupom).
- Proceduralne skripte za optimizaciju servera sa sistemom za obaveštavanje administratora nakon izvršavanja – dnevni uvid na potrošnju resursa i stanje trenutno pokrenutih servisa nakon optimizacije.
- Kompletan sistem obaveštavanja kada su u pitanju sigurnosni i aplikativni aspekti: uspešno prijavljivanje na server sa nove autorizovane IP adrese, statistika sprečenih napada na server, urgentno obaveštavanje ukoliko dođe do pada prethodno definisanih servisa od krucijalnog značaja za normalno funkcionisanje servera.
- Na serveru je namešteno automatsko ažuriranje centralnog dela operativnog sistema (*Kernel*) kao i svih aplikacija od kojih se zahteva da budu u režimu stalne nadogradnje – na ovaj način se postiže najviši nivo sigurnosti primenom najnovijih zakrpa. Dostupnost servera je na nivou od 99+%. Ova dostupnost nije zagarantovana već trenutna i ciljana.

Provajderi servera i lokacija: Hetzner Online (Falkenstein/Vogtland, EU Germany), Amazon (Frankfurt, EU Germany)

Korišćeni infrastrukturni provajderi Hetzner Online GmbH i Amazon Web Services (AWS) primenjuju međunarodno priznate standarde zaštite podataka i informacione bezbednosti, uključujući GDPR usklađenost i ISO 27001 sertifikaciju.

Hetzner Online GmbH:

- GDPR Data Processing Agreement (DPA): https://www.hetzner.com/AV/DPA_en.pdf
- Data Protection & GDPR informacije: <https://docs.hetzner.com/general/company-and-policy/data-protection-at-hetzner/>
- ISO 27001 sertifikacija: <https://www.hetzner.com/unternehmen/zertifizierung/>
- Technical and Organizational Measures (TOMs): <https://docs.hetzner.com/general/others/technical-and-organizational-measures>

Amazon Web Services (AWS):

- AWS GDPR Data Processing Addendum: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
- AWS Compliance Programs: <https://aws.amazon.com/compliance/programs/>
- AWS ISO 27001 Compliance: <https://aws.amazon.com/compliance/iso-27001-faqs/>
- Amazon S3 Security Best Practices: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html>

Navedeni provajderi posluju u skladu sa evropskim i međunarodnim standardima zaštite podataka, uz primenu tehničkih i organizacionih mera zaštite podataka i informacionih sistema.

Sigurnosne kopije podataka se rade jednom dnevno na fizički udaljeni server kojem može da se priđe isključivo iz podmreže servera čime se postiže najviši nivo zaštite kako u softverskom tako i u hardverskom smislu (prirodne nepogode, fizički i ssh pristup, kvar na serveru itd...).

Backup proces se obavlja korišćenjem savremenih alata, čime se obezbeđuje pouzdana redundansa i maksimalna sigurnost podataka. Politika čuvanja predviđa da se backupi zadržavaju do 24h unazad. U slučaju gubitka podataka, bilo usled tehničkog kvara, greške, neovlašćenog pristupa ili prirodne katastrofe, kompanija će obaviti potpuno vraćanje korisničkih podataka u roku od 72 časa od trenutka incidenta.

Sistem za vraćanje podataka se redovno testira kroz planske simulacije katastrofa (disaster recovery drills), kako bi se osigurala spremnost u realnim situacijama.

Politika čuvanja podataka je u skladu sa važećim zakonima o zaštiti podataka i internim bezbednosnim standardima kompanije. Kompanija se obavezuje da prati promene u zakonskoj regulativi i po potrebi prilagođava ovu politiku.

Uvek ažurna verzija ovog izveštaja se može naći na linku:

<https://kancelarko.rs/izvestaj-o-stanju-servera-kancelarko-rs.pdf>

U Beogradu, dana 14.05.2026.

direktor

Nevena Živanović