

Naziv Zaposlenog: Dejan Nikolić
Bezbednosna Organizacija: Sigurnosni Tim Telekom Srbije
Pogodjena Organizacija: Telekom Srbija
Ozbiljnost Incidenta: kritična
Adresa Pogodjene Organizacije: Bulevar Mihajla Pupina 6, Beograd

Opis incidenta:

U julu 2025. godine, Telekom Srbija se suočio sa ozbiljnim sigurnosnim incidentom koji je uključivao kompromitovanje jednog od njihovih ključnih servera za autentifikaciju korisnika. Napadači su iskoristili ranjivost u zastareloj verziji softvera za pristup sistemu, što im je omogućilo pristup velikom broju korisničkih naloga i osetljivih podataka.

Incident je otkriven kada su korisnici prijavili neobične aktivnosti na svojim računima, uključujući neovlašćene promene podešavanja i pokušaje preusmeravanja poziva. Brzom reakcijom bezbednosnog tima uspelo se da se ograniči dalji pristup i pokrene proces povraćaja kontrole nad ugroženim nalogima.

Sprovedena je dubinska analiza i forenzička istraga kojom su identifikovani izvori napada, kao i korišćene metode eksploatacije. Na osnovu nalaza, uvedeni su hitni bezbednosni patch-evi i kompletna nadogradnja sistema za upravljanje pristupima.

Kompanija je takođe pokrenula obaveštajne kampanje prema korisnicima, upozoravajući ih na moguće rizike i preporučujući korišćenje dvofaktorske autentifikacije. Paralelno sa tim, formiran je tim za kontinuirani monitoring i unapređenje sigurnosne arhitekture.

Ovaj incident predstavlja važan podsjetnik na neophodnost redovnog ažuriranja softvera, stalnog nadzora i edukacije zaposlenih u cilju prevencije budućih sajber pretnji koje bi mogle ugroziti kritične telekomunikacione infrastrukture.