

Case study: JP BH Telekom d.d.



Implementacija Security rješenja u BH Telecom-u

BH Telecom, kao vodeća telekomunikacijska kompanija u BiH, sa velikim brojem korisnika, susreće se sa različitim izazovima u pogledu sigurnosti i zaštite podataka, aplikacija i uređaja unutar interne infrastrukture. Neki od tih izazova su:

- Zaštita od neovlaštenog pristupa podacima
- Zaštita od internih napada i gubitka podataka
- Pojednostaviti usklađenost sa regulatornim standardima (GDPR)
- Prepoznavanje sumnjivih napada i kršenja politike
- Prikupljanje podataka relevantnih za sigurnost kompanije sa različitih izvora kao što su firewall, user directories, proxy, aplikacije, ruteri, itd
- Uvid u ranjivosti cjelokupne infrastrukture te način zaštite od istih

Implementacijom odgovarajućih sigurnosnih rješenja, naš tim pomaže svojim klijentima da savladaju različite sigurnosne izazove. Unutar mreže BH Telecom-a implementirali smo sljedeća rješenja:

- **IBM Security Guardium** - rješenje koje nudi centralizirani set kontrola za monitoring aktivnosti baza podataka u realnom vremenu, detaljan auditing baza podataka, automatiziran reporting, analizu sigurnosti baza podataka, DLAC (Data-Level Access Control) kontrolu, automatsko otkrivanje senzitivnih podataka i mnoge druge opcije.
- **IBM QRadar** - Enterprise rješenje koje objedinjuje podatke od izvora log saobraćaja iz velikog broja uređaja distribuiranih preko mreže, skladištenje svakog podatka u Raw formatu, a zatim korelaciju u cilju razlikovanja stvarnih prijetnji od lažnih. Nudi mogućnost snimanja Layer 4 podataka mrežnog saobraćaja u realnom vremenu, kao i sadržaj Layer 7 aplikacija, koristeći Deep Packet Inspection tehnologije
- **Qualys Vulnerability Management** - cloud-based servis koji omogućava trenutnu, globalnu vidljivost gdje IT sistemi mogu biti ugroženi od strane najnovijih Internet prijetnji i kako ih zaštititi od istih. Na ovaj način omogućeno je kontinuirano prepoznavanje različitih prijetnji i nadgledanje neočekivanih promjena u mreži i njihovo pravovremeno otklanjanje.

Glavni zadatak i cilj je bio osigurati integraciju navedenih rješenja, tj. omogućiti pregled ključnih informacija na jedinstvenoj platformi, te na taj način pojednostaviti korištenje navedenih rješenja za krajnjeg korisnika.

IBM QRadar je implementiran kao krovno rješenje koje prikuplja informacije iz svih segmenata IT infrastrukture te je izvršena integracija sa IBM Security Guardium i Qualys VM rješenjima.

Implementacijom i integracijom navedenih rješenja osigurana je zaštita IT sistema i podataka u mreži BH Telecoma kao i omogućeno pravovremeno djelovanje na potencijalne prijetnje, zlonamjernu manipulaciju podacima te saniranje otkrivenih ranjivosti.