Informacija o realizaciji nabavke opreme za Disaster Recovery lokaciju glavni data centar dio za mrežu i bezbednost

Jačanje Vladine infrastrukture i ključnih segmenata jedinstvenog informacionog sistema u skladu sa Zakonom o elektronskoj upravi permanentni su prioriteti u 2021. godini. Stanje serverske i mrežne opreme u Data centru značajno je unaprijeđeno u tekućoj godini, posebno segment serverske opreme.

Programom rada Vlade za 2021. godinu jedan od prioriteta u radu Ministarstva javne uprave, digitalnog društva i medija predstavlja jačanje mrežne i sigurnosne opreme u mreži državnih organa, u smislu obezbjeđivanja većeg nivoa informacione bezbjednosti, pune dostupnosti Vladinih servisa i informacionih sistema.

Zakon o elektronskoj upravi definisao je da elektronska uprava funkcioniše preko jedinstvenog informacionog sistema organa, informaciono-komunikacione mreže organa i sistema za elektronsku razmjenu podataka, kao i preko informacionih sistema koje uspostavljaju organi i drugi subjekti.

U Data centru Ministarstva javne uprave, digitalnog društva i medija su hostovani načelno svi ključni servisi kojima pristupaju korisnici mreže državnih organa (mail server Vlade, aktivni direktorijum Vlade), kao i važni informacioni sistemi (eDMS, Portal Vlade, Portal eUprave, Elektronske sjednice Vlade, JISERP – jedinstveni informacioni sistem za razmjenu podataka i dr.).

Pored brojne opreme za sisteme i servise koje održava Ministarstvo javne uprave, digitalnog društva i medija u Data centru se hostuje i oprema za potrebe projekata i drugih institucija. Razlog pređašnjeg stava formiran je na osnovu stava da navedene institucije nemaju razvijenu ICT infrastrukturu i obezbijeđen prostor koji bi zadovoljio standarde za ovu namjenu i to:

1. Ministarstvo finansija i socijalnog staranja – informacioni sistemi za centralizovani obračun zarada i planiranje budžeta;
2. Ministarstvo javne uprave, digitalnog društva i medija u saradnji sa Ministarstvom unutrašnjih poslova - registracija novorođenih/preminulih, promjena adrese prebivališta, uvid u katastar (online plaćanje poreza), online prijava za vjenčanja i izdavanje potvrde;
3. Ministarstvo zdravlja – informacioni sistema za izdavanje digitalnih covid potvrda;
4. Ministarstvo prosvjete, nauke, kulture i sporta – portal za streaming video mateijala u okviru projekta uči doma, portal etičkog komiteta;
5. Ministarstvo ekomskog razvoja – portal za turističke vaučere, portal javnih nameta;
6. Ministarstvo poljoprivrede, šumarstva i vodoprivrede – informacioni sistem evidencije poljoprivrednih gazdinstava (prihodi i rashodi);
7. Ministarstvo kapitalnih investicija – aplikacija za share printera;
8. Uprava za kadrove - informacioni sistem kadrovske evidencije i platforma za učenje Ilias;
9. Agencija za zaštitu konkurencije – informacioni sistema za mjere državne pomoći ekonomiji u toku pandemije COVID19;

10. Agencija za investicije Crne Gore – portal institucije;
11. Predsjednik Crne Gore – portal institucije;
12. Uprava za dijasporu – registar raseljenih lica;
13. Komisija za kontrolu postupka javnih nabavki – portal institucije i portal javnih nabavki.

Osnovna karakteristika Data centra je smještaj ključnih serverskih i storage resursa na kojima su podignute sve aplikacije i aplikativni servisi. Zbog toga je brza i efikasna pristupna mreža za servere centralna karakteristika ovog dijela mreže.

Serverski segment je dizajniran sa ciljem da se:
- Obezbijedi maksimalno smanjenje kašnjenja saobraćaja prema serverima i saobraćaja između servera;
- Da se obezbijede adekvatne mrežne inter-konekcije sa MAN i WAN mrežnim segmentima;
- Omogući visoka dostupnost mrežne topologije i otpornost na otkaze hardvera i softvera;
- Obezbijedi visoka gustina portova kako bi mrežna infrastruktura mogla da podrži proširenje broja servera i servisa u mjeri u kojoj se to zahtijeva od iste;
- Obezbijedi fleksibilnost i sposobnost prilagođavanja različitim zahtjevima koji se mogu javiti tokom perioda eksploatacije.

Ovakav dizajn serverskog pristupnog segmenta omogućava visoke performanse kako standardnih tako i virtualizovanih okruženja sa virtualizacionim platformama poput VMWare.

Realizacijom ove aktivnosti omogućila se implementacija adekvatne mrežne topologije i tako implementira dobar nivo zaštite i logičkog razdvajanja, kao i visoke perfomanse na L2 i L3 nivou koje bi omogućile da se koriste varijante sistema za zaštitu poput naprednih L7 firewall sistema, WAF sistema, IPS/IDS sistema i slično.

Realizacija ovih aktivnosti predstavlja osnovni preduslov za dalji razvoj e-uprave i proces digitalizacije države i iz tog razloga realizovane su aktivnosti:

1. Opremanje hardverom Data centra Ministarstva javne uprave, digitalnog društva i medija u cilju unaprijeđenja segmenta informacione bezbjednosti u data centru i mreži organa državne uprave;
2. Opremanje Disaster recovery centru u Bijelom Polju;

Prva aktivnost, kao što je prethodno davedeno se odnosi neophodne procese u cilju povećanja stepena informacione bezbjednosti u smislu neovlaštenog pristupa podacima, sajber napada i dostupnosti servisa kroz nabavku i implementaciju infrastrukturne opreme u Data centru, Ministarstva javne uprave, digitalnog društva i medija, i to redudantnih bezbjednosnih firewall uređaja neophodnih za kontrolu saobraćaja na mreži državnih organa i aktivne mrežne opreme koja treba obezbijediti punu redudantnost na core sistemu mreže državnih organa i na taj način onemogućiti ispade u radu sistema a samim tim i punu dostupnost u radu državnih organa. Realizacijom ove aktivnosti dodatno se ojačao kvalitet i brzina prenosa podataka u

mreži državnih organa, kao i bezbjednost podataka, te su se se omogućili dodatne kapaciteti backup-a podataka u ključnim sistemima.

U 2021. godini je u potpunosti implementiran sistem Disaster Recovery servisa na Disaster Recovery lokaciji u Bijelom Polju što je i obaveza Ministarstva koja proizilazi iz Zakona o elektronskoj, pa samim tim predstavlja jednu od ključnih aktivnosti koja je uspješno realizovana u tekućoj godini.

U cilju daljeg unapređivanja mreže državnih organa planirana su sredstva za nabavku aktivne mrežne opreme koja će biti instalirana na pristupnim tačkama u drugim državnim institucijama.

Projekat obuhvata potpunu rekonstrukciju Disaster recovery centra u Bijelom Polju u kome je bilo potrebno omogućiti da se ključni Vladini servisi i sistemi mogu oporaviti u slučajevima elementarnih nepogoda, za potrebe rezervnih kopija informacionih sistema i podataka.

Pored Ministarstva javne uprave, digitalnog društva i medija ovu lokaciju su do sada koristitili:

- Poreska uprava,
- Ministarstvo finasija i socijalnog staranja,
- Investiciono razvojni fond,
- Ustavni sud.

Nakon realizacije projekta Disaster Recovery servisa svi sistemi hostovani na Goverment Cloud platformi su izreplicirani (iskopirani) na Disaster Recovery lokaciju, što je doprijnijelo da se tokom 2021. broj institucija koje koriste usluge Disaster Recovery servisa i Disaster Recovery lokacije povećao sa 4 na 18 institucija.

Ovaj projekat se sprovodio u kontinuitetu i u ranijem periodu za potrebe Disaster recovery lokacije Ministarstvo javne uprave, digitalnog društva i medija je povećalo kapacitete za povezivanje Data centra i Disaster recovery centra optičkim linkom na 1GB za potrebe realizacije servisa, što je uvećanje kapaciteta za 50 puta u odnosu na raniji period, kao jedan od najbitnijih preduslova za replikaciju podataka.

Korisnici Vladinog cloud sistema nemaju potrebu da nabavlju opremu za Disaster Recovery lokaciju, već su po automatizmu korisnici Disaster Recovery servisa i samim tim je obezbjeđen kontinuitet rada informacionih sistema u slučaju nepogoda.

Jedan od ključnih ciljeva Ministarstva je, svakako, digitalizacija javne uprave i crnogorskog društva u cjelini. Samim tim, kao organ državne uprave nadležan za razvoj informacionog društva i elektronske uprave, Ministarstvo ima zadatak da obezbjedi stabilno i sigurno funkcionisanje svih informacionih sistema u njenoj nadležnosti i obezbjedi rezervne kopije podataka istih u slučaju elementarnih nepogoda. Pored toga, u slučaju kada se informacioni sisitemi suočavaju sa sve većom količinom i sve sofisticiranijim sajber napadima, dužnost i obaveza Ministastva je da obezbjedi što veću zaštitu državnih podataka, djeluje proaktivno i pravovremeno u tom cilju.

Benefiti koji su ostvareni realizacijom ove aktivnosti:

- Ministarstvo je u mogućnosti da da obezbjedi sigurnost i bezbjednost mreže organa državne uprave i bezbjednost kopija podataka u skladu sa sigurnosnim standardima;
- Ministarstvo je u mogućnosti da obezbjedi dostupnost mreže organa državne uprave;
- Znatno veća otpornost aktivne mrežne opreme na ispade u slučaju sajber napada;
- Ministarstvo je u mogućnosti da da obezbjedi kontinuitet poslovanja u slučaju elementarnih nepogoda.