Informacija o izradi Studije izvodljivosti o potrebi izgradnje Državnog Data Centra

Ministarstvo javne uprave, kao organ uprave koji je shodno Uredbi o organizaciji i načinu rada državne uprave („Sl. list CG“, br. 49/22, 52/22, 56/22, 82/22, 110/22 i 139/22), između ostalog, zadužen za razvoj informacionog društva i elektronske uprave, vrši poslove uprave koji se odnose na upravljanje Jedinstvenim informacionim sistemom i obezbjeđivanje tehničkih i drugih uslova za njegovo korišćenje.

Zakonom o elektronskoj upravi („Sl. list CG“, br. 72/19), definisano je da Jedinstveni informacioni sistem čine: Data centar, Disaster Recovery centar, informaciono-komunikaciona infrastruktura, kao i dijeljeni infrastrukturni, aplikativni i internet sistemi.

Ujedno, strateško opredjeljenje Vlade Crne Gore je digitalna transformacija kompletnog društva, što je iskazano u različitim strateškim dokumentima, od kojih se naročito ističu: Strategija digitalne transformacije, Strategija reforme javne uprave i Strategija sajber bezbjednosti.

Kao kredibilna članica NATO-a, Crna Gora je snažno orijentisana na ispunjavanje svih obaveza koje proističu iz članstva u ovom savezu. Na taj način, dajemo značajan doprinos kolektivnoj bezbjednosti, kao i obezbjeđivanju zajedničkog sajber prostora.

Vlada Crne Gore i resorno Ministarstvo javne uprave u proteklom periodu su učinili velike napore na unaprjeđenju ambijenta za adekvatnu sajber bezbjednost, pokrenuvši veliki broj inicijativa za jačanje sajber otpornosti.

Naročito je važno istaći činjenicu da je oformljen Vladin CIRT, kao zasebna organizaciona jedinica u okviru Ministarstva javne uprave, čime je omogućen monitoring kompletne informaciono-komunikacione mreže organa, u režimu 24/7. Uz navedeno, uspostavljen je sajber-bezbjednosni ekosistem, čime je bezbjednost informaciono-komunikacione mreže organa podignuta za značajno veći nivo u odnosu na prethodni period.

Za digitalni razvoj neophodno je jačanje sistema sajber bezbjednosti kome je Vlada dala puni značaj koji će biti dodatno osnažen formiranjem Agencije za sajber bezbjednost, ali i same digitalne infrastrukture, koja je fokus ove informacije i u tom smislu u prethodnom periodu kroz Program ekonomskih reformi Crne Gore za period 2023-2025 je predviđena i mjera koja sadrži aktivnosti na jačanju Sistema sajber otpornosti Crne Gore, kao i uspostavljanju snažne digitalne infrastrukture.

U nadležnosti Ministarstva javne uprave nalazi se upravljanje Data Centrom, u kom su smješteni ključni informacioni sistemi i servisi Vlade:

- EDMS sistem elektronske arhive
- elektronske sjednice Vlade,
- Vladin mail sistem,
- Portal Vlade – Gov.me
- Nacionalni sistem za identifikaciju i autentifikaciju
- Nacionalni sistem za elektronsko plaćanje
- Naconalni sistem za razmjenu podataka između državnih organa - GSB
- portal e - uprave,
- portal e - peticije,

- portal nevladinih organizacija,
- portal otvorenih podataka

kao i brojni informacioni sistemi svih ministarstava i organa državne uprave.

Nakon sajber napada na Vladinu infrastrukturu od 20.08.2022. godine, državne insitucije su u skladu sa preporukama najbolje prakse u sličnim situacijama obratile Ministarstvu javne uprave za pomoć. S tim u vezi, zahtjeve za korištenje virtuelizacione platforme Vlade Crne Gore koristi više institucija u odnosu na period prije sajber napada i to:

- Ministarstvo ekonomije za:

    - web portal programi.gov.me,
    - web portal za centralni turistički registar,
    - web portal za podršku malim i srednjim preduzećima,
    - informacioni sistem za patentni registar,
    - web portal jedinsvena kontakt tačka (portal Point Of Single Contact), Montenegro Village portal;

- Ministarstvo kapitalnih investicija za informacioni sistem za monitoring i uštedu energije;
- Ministarstvo nauke za registar subjekata inovacione djelatnosti i veb portal za programe podrške inovacijama;
- Ministarstvo evropskih poslova za veb portal za IPA projekte;
- Uprava za kadrove za informacioni sistem za elektronsko testiranje kandidata;
- Predsjednik Crne Gore za novi web portal institucije;
- Uprave za inspekcijske poslove za jedinstvei inspekcijski informacioni sistem i portal za zaštitu potrošača.

Dakle, radi se o broju od 7 institucija i 14 novih informacionih sistema, koji su implementirani na Vladinoj cloud platformi nakon sajber napada, čime dolazimo do ukupnog broja od 46 informacionih sistema i 23 državnih institucija, koji se nalaze na preko 170 virtuelnih servera.

Svi sistemi nalaze se na virtuelizacionoj platformom u okviru jedinstvenog Vladinog private cloud sistem. Ovakva serveska struktura je preduslov da bi se povoljnosti novih tehnologija iskoristile u punom kapacitetu koje u krajnjem rezultira brojnim benefitima. Ovakav pristup je u potpunosti obezbjedio mogućnost državnim organima da prilikom kreiranja informacionih sistema i registara koriste infrastrukturu Vladine private cloud platforme, bez ikakvih troškova u smislu kupovine hardvera, licenci i sistemskog softvera, što predstavlja bitan segment racionalizacije finansijskih sredstava.

Dodatnu pogodnost ovakvog postupanja donosi smanjenje drugih troškova za državne organe, a odnose se na održavanje opreme, koji nijesu mali, a nerijetko se kreću u iznosu od 10-15% na godišnjem nivou od vrijednosti same opreme.

Ukupne uštede u odnosu na korišćenje centralizovanog načina čuvanja podataka i hostovanja informacionih sistema okvirno iznosi 700,000€ samo na opremi, a ukoliko bi tome dodali i pružanje usluga upotrebom softverskih alata za sajber bezbjednost te usluge

održavanja opreme, platformi, alata ova cifra bi aproksimativno iznosila i do 1.500.000 eura.

Takođe, stepen informacione bezbjednosti u smislu neovlaštenog pristupa podacima, dostupnosti i sajber bezbjednosi servisa, je mnogo veći, jer je oprema smještena u Data centru, a Ministarstvo javne uprave posjeduje određene bezbjedonosne sisteme i alate i znanje, kao i kadrovske kapacitete koje su unapređuju u kontinuitetu, koje ponaosob svi državni organi ne mogu obezbjediti.

Takođe, potrebno je i unaprijediti kvalitet uslova na Disaster Recovery lokaciji, koja se trenutno nalazi u Bijelom Polju , na kojem ovo ministarstvo u kontinuitetu radi kako bi se svi navedeni sistemi redovno replicirali u realnom vremenu, te da bi u slučaju elementarne nepogode koja bi zadesila primarni Data centar, svi sistemi mogli nastaviti nesmetano funkcionisanje, do potpunog oporavka primarne lokacije.

Uz Data centar kojim upravlja Ministarstvo javne uprave, jedan manji broj državnih institucija posjeduje sopstvene data centre, koji su u potpunosti fizički odvojeni i nalaze se na različitim lokacijama.

Važno je istaći da Ministarstvo javne uprave posjeduje dovoljno infrastrukturnih resursa koji se mogu iskoristiti za potrebe organa državne uprave. Takođe u okviru Data centra ministarstva jhavne uprave implementirani su sistemi :

- Tehnički sistemi zaštite(vido nadzor, kontrola pristupa)
- Agregatsko napajanje
- Sistema za rezervno napajanje i stabilizaciju naposa UPS
- Rana detekcija požara
- Protivpožarni sistem,

kao i čitav set bezbjedosnosnih alata koji čine sajber ekosistem.

Međutim, Data centar kojim upravlja ovo ministarstvo ne ispunjava stroge standarde Tier3+ u smislu da se nalazi u namjenskom posebnom objekta predviđene udaljenosti od određenih trasa , njegove poveznosti na dva različita energetska izvora.

Za razliku od Data centra Ministarstva javne uprave, data centri pojedinih institucija ne zadovoljavaju ni minimalne uslove koje treba da imaju implementirane savremeni data centri, pa samim tim nije moguće u potpunosti uspostaviti ni sve mjere informacione i sajber bezbjednosti.

Postojanje većeg broja zasebnih data centara u okviru državne administracije prouzrokuje neracionalno trošenje novčanih sredstava na državnom nivou, budući da je, u skladu sa svim međunarodnim standardima iz ove oblasti, nakon nekoliko godina neophodno vršiti promjenu postojećih serverskih i informaciono-komunikacionih uređaja. Uz navedeno, za svaki od data centara se vrši utrošak električne energije pojedinačno, kao i novčanih sredstava za održavanje svih bezbjednosnih sistema u okviru istih, što dodatno predstavlja finansijsko opterećenje za državu.

Uzimajući u obzir navedeno, a u cilju obezbjeđivanja neophodnih preduslova za dalju digitalnu transformaciju crnogorskog društva, neophodno je otpočeti aktivnosti na planiranju izgradnje Državnog Data centra, koji bi predstavljao jedinstven kompleks za kompletnu državnu administraciju, a koji bi bio izgrađen u skladu sa svim međunarodnim standardima koji se odnose na data centre, informacionu i sajber bezbjednost. Iako je cilj izgraditi jedan objekat sa dovoljno kapaciteta za potrebe svih državnih institucija, Državni

Data centar bi se mogao segmentirati i obezbijediti organizacija posebnih prostorija za one institucije koje imaju specifične bezbjednosne zahtjeve.

Takođe, Minisatarstvo javne uprave će prilikom pripreme studije izvodljivosti paralelno i obraditi pitanje Disaster Recovery lokacije, i ispunjavanje identičnih standardima kao i primarna lokacija i koja treba posjedovati punu funkcionalnost, kako bi se u realnom vremenu mogli replicirati svi vitalni informacioni sistemi.

Državni Data centar i Disaster Recovery lokacija trebaju biti izgrađeni u skladu sa Tier3+ standardom. Isto podrazumijeva, između ostalog, garantovanu neprekidnu dostupnost i funkcionalnost svih servisa u režimu 24/7/365, ukupni godišnji prekid rada manje od 1,6 sati i redudantnost sistema za neprekidno napajanje i hlađenje. Data centri ovog nivoa su predviđeni za smještanje informacionih sistema koji opslužuju veliki broj korisnika i posjeduju visok nivo informacione i sajber bezbjednosti. Kao takvi, adekvatni su za potrebe državne administracije u Crnoj Gori.

U vezi sa prethodno navedenim, neophodno izraditi Studiju izvodljivosti (engl. Feasibility Study) za izgradnju Državnog Data centra i nove Disaster Recovery lokacije, u okviru koje će se predvidjeti optimalni model finansiranja. Ovo će, ujedno, predstavljati početnu aktivnost i osnovu za sve naredne korake do finalizacije kompletnog projekta. Studija izvodljivosti zahtjeva ekspertsko učešće za koje potrebe je Ministarstvo javne uprave opredijelilo neophodna sredstva.

Ujedno Ministrastvo javne uprave potrebno je da u komunikaciji sa Glavnim gradom, a u skladu sa kriterijumima koji proizilaze iz standarda predvidi Tier3+ dođe do adekvatnog riješenja za buduću lokaciju državnog Data centra.