Informacija o preduzetim aktivnostima povodom saniranja posljedica izazvanih sajber napadima na Vladinu informatičku infrastrukturu i informaciono-komunikacionu mrežu organa

Vladina informatička infrastruktura i informaciono-komunikaciona mreža organa su od 20. avgusta 2022. godine pod kontinuiranim sajber napadima velikog intenziteta i kompleksnosti.

Detaljnom analizom od strane Ministarstva javne uprave utvrđeno je djelovanje ransomware malicioznog koda i detektovani su DDoS i Botnet napadi visokog nivoa sofisticiranosti. U cilju predostrožnosti i sprječavanja daljih posljedica napada, izvršeno je isključivanje servera na kojima su smješteni informacioni sistemi organa, sa informaciono-komunikacione mreže organa.

Uzimajući u obzir činjenicu da je isključivanjem informacionih sistema onemogućena elektronska komunikacija među institucijama, uspostavljeni su privremeni vidovi komunikacije sa IT administratorima u institucijama. Na taj način je obezbijeđeno pravovremeno dijeljenje svih neophodnih informacija, kako bi u što hitnijem roku svi informacioni sistemi na informaciono-komunikacionoj mreži organa bili ponovo funkcionalni.

Tokom analize utvrđeno je da je kriptovano ukupno 17 informacionih sistema u 10 institucija, dok je sajber napad direktno uticao na 150 računara.

Realizovane aktivnosti

U skladu sa definisanim Planom prioritetnih aktivnosti na oporavku Vladine informatičke infrastrukture, preduzete su aktivnosti na uspostavljanju ključnih informacionih sistema neophodnih za nesmetano funkcionisanje državne uprave i servisa koji se pružaju građanima i to:

- konfigurisan je u potpunosti novi javni DNS servis, neophodan za funkcionisanje svih web aplikacija;
- faznim oporavkom Vladine informatičke infrastrukture uspostavljena je elektronska komunikacija između servisa u organima državne uprave, u cilju isplate dječijih dodataka i socijalnih davanja;
- rekonfigurisane su direktne VPN konekcije između institucija, u cilju nesmetane upotrebe informacionih sistema Ministarstva finansija, prvenstveno za upravljanje javnim finansijama;
- obezbijeđen je u potpunosti novi internet link od strane provajdera, namijenjen za ponovno uspostavljanje prioritetnih servisa i dostupnosti putem interneta;
- uspostavljen je portal e-uprave u okviru koga se vrši elektronska prijava stručnog osposobljavanja lica sa stečenim visokim obrazovanjem. Naime, na postojećem informacionom sistemu je ustanovljen značajan bezbjednosni rizik, pa su pokrenute aktivnosti na izradi novog rješenja koji će se isti prevazići;
- uspostavljen je Elektronski sistem javnih nabavki (CEJN) i time obezbijeđeno nesmetano funkcionisanje procesa javnih nabavki u Crnoj Gori;
- u cilju potpune transparentnosti i komunikacije sa građanima i privredom, ponovo je dostupan Vladin portal gov.me, dok je za potrebe oglašavanja radnih mjesta obezbijeđeno nesmetano funkcionisanje informacionog sistema Uprave za ljudske resurse;

- ponovo je uspostavljen Portal elektronskih sjednica Vlade (eSV);
- ponovo je uspostavljen Sistem za elektronsku razmjenu dokumenata (eDMS);
- izvršena je rekonfiguracija Aktivnog direktorijuma i njegovo ponovno uspostavljanje, u cilju omogućavanja rada domenskih radnih stanica, kao i korporativnog antivirusnog rješenja na njima;
- konfigurisan je novi Exchange server za potrebe funkcionisanja službenih e-mail adresa i nesmetano odvijanje poslovne korespondencije. Važno je istaći da je Ministarstvo javne uprave uspješno sačuvalo mailbox-ove svih korisnika i da su isti trenutno stavljeni van funkcije, do sticanja uslova za njihovu ponovnu upotrebu;
- osposobljeni su i servisi drugih državnih institucija i to:
    - Ministarstva pravde (Registar novčanih kazni i prekršajne evidencije),
    - Agencije za nacionalnu bezbjednost (e-mail server),
    - Ministarstva prosvjete (elektronski upis u studenske i đačke domove) i
    - portal Državnog tužilaštva Crne Gore (tuzilastvo.me).

Aktivnosti u toku

Izvršen je oporavak i u toku je finalno testiranje sljedećih informacionih sistema:

- Informacioni sistem za elektronsko plaćanje (NS-NAT) i Informacioni sistem za identifikaciju (NS-eID), koji su u nadležnosti Ministarstva javne uprave;
- Jedinstveni inspekcijski informacioni sistem (JISS) i portal potrosac.me, koji su u nadležnosti Uprave za inspekcijske poslove;
- Kadrovski informacioni sistem (KIS), u nadležnosti Uprave za ljudske resurse.

Važno je istaći da su Ministarstvu javne uprave, u smislu oporavka od sajber napada, pored domaćih, podršku pružili i međunarodni partneri. Ekspertski tim iz Sjedinjenih Američkih Država pružio je stručnu (konsultativnu) podršku u prevazilaženju novonastale situacije i planiranju i stvaranju mehanizama za adekvatniju sajber odbranu/zaštitu u slučaju novog sajber napada visokog nivoa sofisticiranosti. Od strane eksperata iz Republike Francuske, odnosno Nacionalne agencije za bezbjednost informacionih sistema (ANSSI), Ministarstvu je pružena podrška na ponovnom uspostavljanju pojedinih informacionih sistema. Sa partnerima iz Velike Britanije razmijenjena su iskustva u vezi aktuelnih sajber napada i planirani su zajednički projekti za unapređenje informacione bezbjednosti u Crnoj Gori.

Takođe, Ministarstvo javne uprave, uz podršku Ženevskog centra za upravljanje sektorom bezbjednosti (DCAF), kroz angažovanje eksperta iz oblasti sajber bezbjednosti, započelo je aktivnosti na izradi novog Zakona o informacionoj bezbjednosti koji će biti usklađen sa EU regulativom i u kojem će se prepoznati mehanizmi za jačanje sajber bezbjednosti u Crnoj Gori.

U cilju bolje organizacije sajber bezbjednosti na nivou mreže organa državne uprave kojom upravlja Ministarstvo javne uprave, u toku je formiranje posebne organizacione jedinice u vidu Direkcije za informacionu bezbjednost koja će djelovati u okviru Vladinog bezbjednosno-operativnog centra (Government Security Operations Center - GSOC).

Uspostavljen je napredni ekosistem sajber bezbjednosti i implementiran skup alata potrebnih za efikasan sistem detekcije, odgovora na prijetnje i prevencije štete nad imovinom i podacima.

Napredni ekosistem sajber bezbjednosti obuhvata niz unapređenja, koja se odnose na:

- centralizovano upravljanje alatima, kao jedinstveno administrativno rješenje u kojem su integrisane sve komponente bezbjednosnih operacija, u cilju omogućavanja potpune efikasnosti i vidljivosti u cijelom ekosistemu, kao i kontrolu nad svim incidentima, od upozorenja do otklanjanja. U okviru ovog alata nalaze se i funkcionalnosti rješenja za prikupljanje sigurnosnih informacija i događaja (SIEM), koji pružaju kompletan uvid na cjelokupnu IT infrastrukturu;
- napredno endpoint rješenje za anti-virus, anti-spam i anti-malware zaštitu krajnjih uređaja (računara i servera);
- zaštitu elektronske pošte, u vidu skupa komercijalnih alata (e-mail gateway, sandboxing, antivirus), koja zaustavlja prijetnje koje se prenose putem e-pošte, uz identifikaciju napada i napadača, prije nego što prouzrokuju štetu;
- alate za analizu, u cilju otkrivanja napada sa visokom preciznošću i niskom stopom lažnih upozorenja, kao i otkrivanja i zaustavljanja napada na mrežnom nivou;
- alate za pretragu fajlova i mrežnog saobraćaja, kao i mapiranje procesa iz sistema u realnom vremenu, brisanje i zaustavljanje malicioznih procesa u sistemu po indikatorima kompromitacije (IOC);
- alate za provjeru nepoznatih prijetnji sa mehanizmom za dinamičku analizu bez potpisa koji provjerava sumnjivi mrežni saobraćaj;
- alate za praćenje globalnih sajber kampanja u cilju proaktivnog djelovanja i otklanjanja poznatih ranjivosti na sistemima;
- alate za monitoring mrežnih uređaja, servera i detekciju upozorenja na istim;
- alate za skeniranje portala i informacionih sistema na poznate ranjivosti;
- web aplikativni firewall za zaštitu web portala;
- serverski firewall unaprijeđen dodatnim sistemima zaštite od neovlašćenog pristupa serverskoj infrastrukturi;
- internet firewall za kontrolu kompletnog mrežnog saobraćaja sa funkcionalnostima za nezavisnu administraciju do 250 mrežnih lokacija;
- dvofaktorsku autentifikaciju udaljenih VPN konekcija.

Pored implementacije prethodno navedenih alata, izvršena je bezbjednosna organizacija Aktivnog direktorijuma, na koji se oslanja Vladin e-mail sistem, kako bi se dostigao viši stepen sajber zaštite. U skladu sa navedenim, sprovedene su sljedeće aktivnosti:

- aktivni direktorijum je organizovan u bezbjednosne zone, nad kojima se primjenjuju kompleksne bezbjednosne politike;
- izvršena je reorganizacija korisničkih naloga na način što su uklonjeni svi neaktivni nalozi i radne stanice;
- unaprijeđene su politike definisanja kompleksnosti korisničkih lozinki i intervala obavezne promjene istih;
- onemogućen je udaljeni pristup Aktivnom direktorijumu, dok je administracija istog moguća isključivo sa uređaja koji se namjenski koriste u tu svrhu.

Dalje, u cilju postizanja višeg stepena informacione bezbjednosti u mreži državnih organa, Ministarstvo javne uprave je implementiralo određeni broj bezbjednosnih softverskih paketa, koji zahtijevaju hardverske karakteristike računara novije generacije. Shodno tome, računari sa 32-bit procesorskim jedinicama i operativnim sistemima starijim od verzije Windows 10 (u 64-bit varijanti) uslijed nekompatibilnosti sa naprednim alatima sajber zaštite, neće se moći

koristiti na mreži državnih organa, te je iste potrebno zamijeniti u što kraćem roku. Procjenjuje se da broj računara koje je iz navedenih razloga potrebno zamijeniti nije veći od 200.

U cilju preduzimanja mjera i aktivnosti za otklanjanje posljedica sajber napada i sprječavanje nastanka novih, Operativni tim za suprotstavljanje sajber napadima donio je preporuke i mjere u više navrata, koje su dostavljene svim organima državne uprave. Shodno navedenom, organi su, u koordinaciji sa službenicima Ministarstva javne uprave, u prethodnom periodu radili na oporavku korisničkih računara.

Naime, reinstalacijom operativnih sistema svih računara u mreži organa državne uprave i njihovim učlanjenjem u domen, stvaraju se preduslovi za obezbjeđivanje pristupa internetu. Službeni računari su reinstalirani na način koji će omogućiti automatizovan proces dostavljanja bezbjednosnih ažuriranja u narednom periodu. Takođe, u nove operativne sisteme je integrisan korporativni sistem antivirusne zaštite, kojim se upravlja i vrši monitoring centralizovano, u cilju pravovremene reakcije na buduće sajber incidente.

Takođe, shodno navedenim preporukama i mjerama Operativnog tima, službenicima nije dozvoljeno da nakon reinstalacija računara izvrše vraćanje podataka, do sticanja uslova za isto. Ministarstvo javne uprave će u narednom periodu obezbijediti potrebne serverske resurse i alate za potrebe skeniranja prethodno arhiviranih podataka. Na taj način će se mogućnost ponovne infekcije prethodno reinstaliranih uređaja i informaciono-komunikacione mreže organa svesti na minimum.

Do ovog momenta, od ukupno 2471 računara koje je potrebno reinstalirati, reinstalacija je izvršena na 1059, od čega su službenici Ministarstva javne uprave izvršili ukupno 550 reinstalacija. Od ukupnog broja reinstaliranih računara (1059), njih 909 je učlanjeno u domen.

Naročito je važno istaći da su, iako većina institucija zapošljava službenike iz oblasti IT-a, službenici Ministarstva javne uprave pružali podršku u smislu kreiranja rezervnih kopija podataka, reinstalacija računara i učlanjivanja istih u domen i u ovim institucijama, što je iziskivalo ulaganje dodatnih napora službenika ovog ministarstva, a sve u cilju bržeg prevazilaženja novonastale situacije.

Prikaz broja reinstaliranih računara, po institucijama, predstavljen je u sljedećoj tabeli.

Naziv institucije	Ukupan broj računara	Broj reinstaliranih računara	Broj računara učlanjenih u domen	Reinstalirani računari od strane MJU	Broj računara uklonjenih sa mreže ODU
Generalni sekretarijat Vlade Crne Gore	180	128	110	115	1
Ministarstvo ekologije, prostornog planiranja i urbanizma	248	35	6	-	3
Ministarstvo ekonomskog razvoja i turizma	190	95	87	-	-
Ministarstvo evropskih poslova	100	70	46	-	-
Ministarstvo finansija	160	35	35	35	-
Ministarstvo javne uprave	100	92	92	92	9
Ministarstvo kapitalnih investicija	90	87	68	35	10
Ministarstvo kulture i medija	32	20	20	10	1
Ministarstvo ljudskih i manjinskih prava	20	15	15	20	3
Ministarstvo nauke i tehnološkog razvoja	23	23	23	-	4
Ministarstvo poljoprivrede, šumarstva i vodoprivrede	160	150	54	74	3
Ministarstvo pravde	75	-	-	-	-
Ministarstvo prosvjete	95	51	48	-	2
Ministarstvo rada i socijalnog staranja	60	49	43	-	3
Ministarstvo sporta i mladih	34	28	28	-	2

Naziv institucije	Ukupan broj računara	Broj reinstaliranih računara	Broj računara učlanjenih u domen	Reinstalirani računari od strane MJU	Broj računara uklonjenih sa mreže ODU
Ministarstvo unutrašnjih poslova i Uprava policije	290	50	40	-	-
Ministarstvo zdravlja	63	49	49	40	1
Agencija za investicije	30	-	-	30	-
Agencija za mirno rješavanje radnih sporova	26	-	-	-	-
Agencija za zaštitu konkurencije	26	25	25	12	2
Direkcija za zaštitu tajnih podataka	23	-	-	-	-
Disciplinska komisija	12	-	-	-	-
Komisija za zaštitu prava u postupcima javnih nabavki	22	9	9	22	-
Komisija za žalbe	9	-	-	-	-
Predsjednik Crne Gore	28	9	9	9	-
Sekretarijat za zakonodavstvo	20	18	-	18	-
Tržišna inspekcija	11	-	-	-	-
Uprava javnih radova	35	-	-	-	-
Uprava za bezbjednost hrane, veterinu i fitosanitarne poslove	54	40	40	10	6
Uprava za dijasporu	15	-	-	-	-
Uprava za inspekcijske poslove	68	45	27	4	-
Uprava za ljudske resurse	44	40	32	-	-
Uprava za saobraćaj	37	37	37	24	-
Uprava za vode	10	-	-	-	-
Zaštitnik imovinsko-pravnih interesa	26	-	-	-	-
Zavod za školstvo	56	-	-	-	-
UKUPNO	**2471**	**1200**	**943**	**550**	**50**

Određeni broj državnih institucija, zbog prioritetnijih obaveza, nijesu uspjele da izvrše reinstalaciju korisničkih računara. Primjeri ovih institucija su: Ministarstvo unutrašnjih poslova i Uprava policije (usljed obaveza po osnovu organizacije lokalnih izborima) i Ministarstvo finansija (uslijed obaveza po osnovu planiranja budžeta). Ministarstvo javne uprave je sa navedenim institucijama u stalnoj komunikaciji, u cilju planiranja daljih aktivnosti.

Institucijama koje su samostalno ili u saradnji sa Ministarstvom javne uprave uspješno izvršile reinstalaciju korisničkih računara i iste učlanile u domen isu.gov.me, omogućen je pristup internetu i na taj način obezbijeđeno nesmetano obavljanje poslovnih procesa.

Pristup internetu je omogućen sljedećim institucijama:

- Generalni sekretarijat Vlade (zgrada Vlade Crne Gore),
- Ministarstvo javne uprave, Ministarstvo poljoprivrede, šumarstva i vodoprivrede, Ministarstvo zdravlja, Ministarstvo rada i socijalnog staranja, Ministarstvo kapitalnih investicija, Ministarstvo ekonomskog razvoja i turizma, Ministarstvo nauke i tehnološkog razvoja (institucije u zgradi „Vektra“),
- Ministarstvo pravde,
- Ministarstvo sporta i mladih,
- Ministarstvo kulture i medija,
- Agencija za zaštitu konkurencije,
- Uprava za saobraćaj.