R E P U B L I K A H R V A T S K A
PRIMORSKO-GORANSKA ŽUPANIJA
GRAD RIJEKA
Gradonačelnik
KLASA: 023-01/19-04/141-55
URBROJ: 2170/01-15-00-19-7
Rijeka, 12. 11. 2019.

Gradonačelnik je 12. studenog 2019. godine donio sljedeći

z a k l j u č a k

1. Zadužuje se Zavod za informatičku djelatnost Grada Rijeka za nadziranje i upravljanje svih parametara i aktivnosti ICT sustava, pravilnika, utvrđenih procedura i propisa u cilju povećanja otpornosti gradske ICT infrastrukture na kibernetičke napade.

2. Nalaže se svim korisnicima gradske elektroničke komunikacijske mreže (MAN) traženje obavezne suglasnosti Zavoda za informatičku djelatnost za bilo kakvo priključenje nove ICT opreme ili aplikativnog rješenja u zajedničku komunikacijsku infrastrukturu Grada Rijeke.

3. Zadužuje se Zavod za informatičku djelatnost da ustroji sustav praćenja aktivnosti korisnika putem kojeg će se sve radnje poduzete na informacijskim sustavima Grada Rijeka bilježiti i pohraniti u zapise (engl. logs).

4. Daje se ovlaštenje Višem savjetniku za informacijsku sigurnost da:

4.1. u slučaju incidenta ili pretpostavljenog incidenta radi osiguranja sigurnosti ICT procesa:

- nadzire primjenu utvrđenih procedura, pravilnika i drugih propisa
- nadzire zapise (logove) o korištenju ICT sustava

4.2. u slučaju utvrđenih nesukladnosti ili pretpostavke o mogućem sigurnosnom incidentu uz informiranje nadređenih i odgovarajuće dokumentiranje:

- izvrši uvid u bilo koji dio ICT sustava,
- prekine radne aktivnosti djelatnika, mrežnih segmenata gradske MAN mreže, poslužitelja ili bilo koju drugu komponentu ICT sustava.

GRADONAČELNIK

REPUBLIKA HRVATSKA - GRAD RIJEKA 1 - PRIMORSKO-GORANSKA ŽUPANIJA - RIJEKA GRADONAČELNIK

mr.s. Vojko OBERSNEL

Dostaviti:
1. Zavod za informatičku djelatnost,
n/r Željka Jurića i Danijela Antonića
2. pročelnicima odjela gradske uprave, svima
3. komunalnim i trgovačkim društvima u vlasništvu Grada, svima
4. ustanovama kojih je osnivač Grad, svima

REPUBLIKA HRVATSKA
PRIMORSKO-GORANSKA ŽUPANIJA
GRAD RIJEKA

Zavod za informatičku djelatnost
KLASA: 650-01/19-02/8
URBROJ: 2170/01-11-00-19-1
Rijeka, 8. studenog 2019.

GRADONAČELNIKU
- o v d j e -

Predmet: Prijedlog zaključka o provedbi mjera kibernetičke i informacijske sigurnosti u incidentnim situacijama

Pročelnik

Željko Jurić

Grad Rijeka, Korzo 16, 51000 Rijeka, Hrvatska
Tel. ++38551209634, Fax. 209635
www.rijeka.hr
E-mail: zeljko.juric@rijeka.hr

Uvod

Područja kibernetičke sigurnosti definirana su u Odluci o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti („Narodne novine“ broj 108/15) i obuhvaćaju sigurnosne mjere u području komunikacijske i informacijske infrastrukture i usluga u kojem razlikujemo javne elektroničke komunikacije, elektroničku upravu i infrastrukturu od primarnog strateškog interesa društva u cjelini. Zakonski okvir u području zaštite osobnih podataka Europske unije također nameće implementaciju tehničkih i organizacijski mjera u zaštiti podatkovne imovine.

Iznimno bitno područje kibernetičke sigurnosti predstavlja i zaštita kritične komunikacijske i informacijske infrastrukture koja se može nalaziti u svakom od prethodna tri infrastrukturna područja koja je na gradskoj infrastrukturi reprezentirana digitalnim servisima pojedinih komunalnih društava te poslovanje elektroničke uprave. Razvoj tehnologije i ovisnost svih segmenata društva o tehnološkom razvoju nije nikad bio tako sveobuhvatan kao što je to u području komunikacijske i informacijske tehnologije. Stvaranjem interneta i povezivanjem niza komunikacijskih i informacijskih sustava javnog, akademskog i gospodarskog sektora te građanstva, stvoren je suvremeni kibernetički prostor. Njega sačinjava povezana infrastruktura u vlasništvu različitih dionika, stalno rastuća količina podataka te korisnici koji međusobno komuniciraju u sve većem broju koristeći rastući broj usluga. Odstupanja od ispravnog rada tih međusobno povezanih sustava ili njihovih dijelova više nisu samo minorne tehničke smetnje, već predstavljaju opasnost većih sigurnosnih razmjera.

Elektronička komunikacijska infrastruktura Grada Rijeke

Zavod za informatičku djelatnost Grada Rijeke (u nastavku Zavod) pruža uslugu Centra dijeljenih usluga, pristupa Internetu te međupovezivanja aktivnom i pasivnom elektroničkom komunikacijskom infrastrukturom Grada Rijeke, komunalnih društava i ustanove kojima je Grad Rijeka osnivač. Zavod je odgovoran i za funkcionalnost, razvoj i sigurnost podatkovnog centra, aktivne i pasivne komunikacijske infrastrukture te podatkovne imovine. Sukladno svojoj nadležnosti Zavod provodi mjere kibernetičke i informacijske sigurnosti u cilju zaštite podatkovne imovine i poslovnih procesa Grada Rijeke, komunalnih društava i ustanova u vlasništvu Grada. Navedeno podrazumijeva implementaciju sigurnosne tehnologije sukladno najboljim praksama te ustrojavanje poslovnih procesa i procedura za korištenje digitalne tehnologije u cilju povećanja dostupnosti, sigurnosti i integriteta podatkovne imovine.

Zavod dnevno pruža usluge pristupa Internetu za prosječno 6.000 uređaja grada, ustanova i komunalnih društava te 1.860 korisnika besplatnog bežičnog pristupa internetu. Za takvu infrastrukturu kibernetički kriminal predstavlja ozbiljnu sigurnosnu prijetnju poslovanju budući je gradski IT sustav svakodnevno izložen izuzetno velikom broju opasnosti koje uključuju maliciozni kod (npr. „cryptoloker“, računalni virusi), pokušaje krađe povjerljivih podataka, napadi na ICT sustave, pokušaje prevara putem socijalnog inženjeringa, Spama, DDOS napada i drugi vrsta opasnosti. Želimo li minimizirati štetu nastalu od takvih aktivnosti, poput širenje malicioznog koda ili zaustavljanje napada na sustav, reakcija na detektirane ugroze mora biti brza, učinkovita i, u pojedinim kritičnim slučajevima, radikalna.

Za navedeno potrebno je ovlastiti stručni kadar za donošenje radikalnih odluka u cilju očuvanja opstojnosti cjelovitog ICT sustava. Dodatno, nužno je osigurati jednaku razinu tehničke usklađenosti, funkcionalnosti i sigurnosti kod svih korisnika gradske elektroničke komunikacijske mreže kako bi se postiglo da svi njeni korisnici imaju isti stupanj sigurnosti podatkovne imovine i funkcionalnosti digitalnih servisa.

Upravljanje informacijskom i kibernetičkom sigurnošću zahtijeva učinkovit sustav za praćenje i kontrolu sumnjivih situacija i sigurnosnih incidenata. Nužna je stalna pozornost i učinkovit sustav upravljanja koji će na efikasan način prepoznati, reagirati i riješiti situacije koje za sobom povlače rizik od narušavanja povjerljivosti, integriteta i dostupnosti informacija.

Slijedom navedenog Zavod ima obavezu istražiti i otkloniti bilo koju situaciju koja je dovela ili predstavlja rizik po integritet, sigurnost ili cjelovitost podataka. Navedeno znači i da Zavod može ograničiti uslugu nekom korisniku ukoliko je to nužno i poduzeti sve potrebne istražne radnje da se ubuduće to ne dogodi ili u slučaju potrebe dostavi nadležnim tijelima sukladno zakonskoj obavezi.

Svaki dio poslovnih procesa Zavoda, poput pristupa internetu, elektroničke pošte, aplikativnih rješenja, radnih stanica, poslužitelja, udaljenog pristupa i drugih digitalnih servisa biti će obuhvaćen sustavom praćenja aktivnosti putem kojih će se sve radnje poduzete informacijskim sustavima Grada Rijeke bilježiti i pohraniti u zapise (engl. logs). Ti su zapisi predmet revizije zbog unaprjeđenja rada sustava i otklanjanja mogućih nesukladnosti.

Slijedom svega navedenog predlaže se Gradonačelniku Grada Rijeke da donese sljedeće:

Z a k lj u č k e

1. Zadužuje se Zavod za informatičku djelatnost Grada Rijeka za nadziranje i upravljanje svih parametara i aktivnosti ICT sustava, pravilnika, utvrđenih procedura i propisa u cilju povećanja otpornosti gradske ICT infrastrukture na kibernetičke napade.

2. Nalaže se svim korisnicima gradske elektroničke komunikacijske mreže (MAN) traženje obavezne suglasnosti Zavoda za informatičku djelatnost za bilo kakvo priključenje nove ICT opreme ili aplikativnog rješenja u zajedničku komunikacijsku infrastrukturu Grada Rijeke.

3. Zadužuje se Zavod za informatičku djelatnost da ustroji sustav praćenja aktivnosti korisnika putem kojeg će se sve radnje poduzete na informacijskim sustavima Grada Rijeka bilježiti i pohraniti u zapise (engl. logs).

4. Daje se ovlaštenje Višem savjetniku za informacijsku sigurnost da:
   4.1. u slučaju incidenta ili pretpostavljenog incidenta radi osiguranja sigurnosti ICT procesa:
      - nadzire primjenu utvrđenih procedura, pravilnika i drugih propisa
      - nadzire zapise (logove) o korištenju ICT sustava
   4.2. u slučaju utvrđenih nesukladnosti ili pretpostavke o mogućem sigurnosnom incidentu uz informiranje nadređenih i odgovarajuće dokumentiranje:
      - izvrši uvid u bilo koji dio ICT sustava,
      - prekine radne aktivnosti djelatnika, mrežnih segmenata gradske MAN mreže, poslužitelja ili bilo koju drugu komponentu ICT sustava.