NALED
Savez za e-upravu
E-Government Alliance

ИЗВЕШТАЈ О ИНФОРМАЦИОНИМ СИСТЕМИМА, ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ И ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ У ЛОКАЛНИМ САМОУПРАВАМА У РЕПУБЛИЦИ СРБИЈИ

Анализа стања у 2019. у односу на 2018. годину и препоруке за унапређење

АПРИЛ 2020.

УРЕДНИЦА
Драгана Илић

АУТОРКА
Ана Миловановић

САРАДНИЦА
Милица Анђелковић Ђоковић

Македонска 30/VII, 11000 Београд, Србија
www.naled.rs

САДРЖАЈ

NALED
Savez za e-upravu
E-Government Alliance

РЕЗИМЕ РЕЗУЛТАТА И ПРЕПОРУКА

АПРИЛ 2020.

ПРЕГЛЕД ОСНОВНИХ РЕЗУЛТАТА ИСТРАЖИВАЊА

Стратешка позиција информационих система

- 19% анализираних локалних самоуправа има Акт о информационој безбедности и доследно га примењује, док га 46% има, али немају контролне механизме примене;
- У 52% локалних самоуправа стратегија развоја информационог система или не постоји или није имплементирана у стратегију развоја локалне самоуправе. У 23% локалних самоуправа је имплементирана делимично, у 4% потпуно, док 4% има засебан документ;
- У 45% локалних самоуправа класификација, обележавање и поступање са информационим добрима према степену осетљивости и критичности није прописана унутрашњим актом.

Људски и технички ресурси локалних самоуправа

- У просеку, једно лице је ангажовано на сваких 62 запослених у локалној самоуправи. У општинама ради 1 ИТ лице на 61 запослених, у градовима је тај однос 1 према 63, а у градским општинама 1 према 59;
- Половина локалних самоуправа запошљава једно ИТ лице са вишом или високом стручном спремом, скоро четвртина два, само 6% три и више. Од 20% локалних самоуправа које не запошљавају уопште лице задужено за ИТ, неке ангажују и екстерне компаније за послове у вези са одржавањем мреже или система;
- 73% локалних самоуправа је одговорило да има мрежног администратора, а 27% да нема уопште или да нема лице које је задужено само за ове послове. Надлежност за управљање информационим системима је најчешће на нивоу одељења (44% локалних самоуправа), одсека (13%), служби (10%) или група (3%), док 26% локалних самоуправа нема посебну организациону јединицу која се бави одржавањем информационих система;
- Општине ће у 2020. години у просеку издвојити 2.977.667 дин, градови 25.605.089 динара и анкетиране градске општине 7.358.250 динара за сервис рачунара и опреме, одржавање постојећих и набавку нових софтвера, нове опреме и осталих трошкова за одржавање система и мреже.
- Број расположивих рачунара у локалним самоуправама углавном кореспондира са бројем запослених или га незнатно надмашује;
- Процентуално највише се користе оперативни системи *Windows 7* (97%) и *Windows 10* (98%), али већина има и одређени број *XP* (62%) или *Linux* оперативне системе (32%). 85% локалних самоуправа користи више оперативних система симултано;

Приступ информационом систему

- Готово је подједнак број локалних самоуправа чији запослени користе лозинке приликом пријављивања на систем и мењају их (49%) и оних чији запослени користе лозинке али их не мењају (50%) Само једна локална самоуправа је пријавила да њени запослени не користе лозинке. Учесталост промене лозинке варира, од једном месечно, квартално, до једном у шест месеци или на годину дана. Негде лозинке мења и сам администратор;
- Поред лозинки, као фактор аутентикације користе се и паметне картице са сертификатом (27% локалних самоуправа) и токени (12%);

- 49% локалних самоуправа не дозвољава коришћење сопствених уређаја запослених за приступ информационом систему. Једнак број омогућава приступ без контроле (23%) и уз коришћење контролних механизама (23%).

Умрежавање рачунара и приступ интернету

- 62% локалних самоуправа наводи да су подаци којима располажу угрожени јер имају приступ интернету (повезаност углавном оптичким каблом). Тек 22% локалних самоуправа сматра да им подаци нису угрожени јер их чувају на посебним рачунарима који немају излаз на интернет или имају антивирус софтвер и *firewall*, док неке наводе да имају приступ интернету путем *proxy* сервера који филтрира дозвољене веб странице када се дефинишу;
- 74% локалних самоуправа сматра да имају крхке делове система, са тендендијама да падну. 26% сматра да су им системи стабилни;
- У 41% локалних самоуправа приступ садржајима на интернету за запослене је неограничен. У 29% је ограничен, док је у 30% делимично ограничен;
- 83% локалних самоуправа користи *WiFi* и *Bluetooth* технологију која је заштићена. Локалне самоуправе које су додале и напомену уз ово питање нагласиле су да је *WiFi* одвојен од локалне мреже која се користи за повезивање запослених на интернет (5 од 5 локалних самоуправа). *WiFi* и *Bluetooth* који нису заштићени користи 6%, док 12% локалних самоуправа наводи да их не користи уопште.

Заштита информационих система

- 44% локалних самоуправа има *firewall* и *IDS/UPS* уређаје, док 35% нема. 16% је навело да их има делимично.Најзаступљенији су *Microtic, Cisco, Microsoft*, као и *Sophos*;
- 93% испитаних локалних самоуправа има антивирус софтвер. 2 локалне самоуправе га немају. Од антивирус софтвера најчешће се користе: *EsetEndpoint, Kaspersky, Avast, SophosEndpoint, MicrosoftSecurityEssentials, WindowsDefender*, а многе користе доступне и бесплатне верзије софтвера;
- Процентуално се у највећем броју локалних самоуправа резервне копије података креирају дневно (67%), те по потреби (42%), затим недељно (39%), а најређи случај је да се резервне копије креирају месечно (25%). 43% локалних самоуправа је на ово питање дало више од два одговора, у зависности о каквим подацима је реч;
- 72% локалних самоуправа прави комплетну резервну копију података. 25% локалних самоуправа креира инкременталне копије, а 20% диференцијалне. 22% локалних самоуправа је нагласило да креира више врста резервних копија података, у зависности од система које користе;
- 81% локалних самоуправа чува резервне копије података на локацији примарног рачунарског центра, 20% локалних самоуправа резервне копије података чува на посебној удаљеној локацији, а 13% на локацији резервног рачунарског центра, док 7% локалних самоуправа резервне копије чува на екстерним хард дисковима или другде. 16% локалних самоуправа је дало два или више одговора на ово питање;
- 70% локалних самоуправа нема резервни рачунарски центар. Тек 3 локалне самоуправе су одговориле да имају пресликани резервни рачунарски центар, 3 да имају *hot site* и 2 да имају *warm.* 15% није дало одговор на ово питање;
- У највећем броју случајева локалне самоуправе које имају резервни рачунарски центар су наводиле исту локацију као за примарни;
- 74% локалних самоуправа је било изложено прекидима у раду услед нестанка струје. Остали фактори који су доприносили прекидима у раду су и

телекомуникациони линкови, мрежна инфраструктура, те главна пословна апликација, мада већина наводи да су сви ови прекиди углавном последица прекида у електричном напајању, редовног одржавања, напада вируса или пада система услед застарелости сервера, рачунара или програма у употреби;

- 47% локалних самоуправа забележило је неки вид напада на информациони систем, 42% наводи да није, док 12% локалних самоуправа не зна да ли је било изложено нападима. Најчешћи су напади на електронску пошту у виду спам мејлова, помоћу малициозних софтвера, потом напади на веб презентације, на рутер и *wifi* мрежу итд;
- Већина локалних самоуправа (58%) није вршила никакву процену безбедности и/или ризика информационих система;
- Ниједна од испитаних локалних самоуправа није тестирала усвојени план опоравка у случају катастрофа у последњих годину дана. 3 су га усвојиле, али нису тестирале у претходних годину дана, а 3 га никада нису тестирале;
- 77% локалних самоуправаје нагласило да организују обуке и подизање свести о информационој безбедности запослених, а 23% да овакве обуке не организује. Оне које су навеле да обуке организују, под тиме подразумевају и одласке на семинаре НАЛЕД-а или давање обавештења запосленима од стране ИТ лица.

Заштита података о личности

- 66% локалних самоуправа не контролише одлив информација из локалне самоуправе. 11% контролише приступ јавним сервисима за размену и чување докумената, 9% електронску пошту, 6% преносиве меморијске уређаје, а 5% приступ јавним сервисима електронске поште;
- Енкрипција осетљивих података се у највећем броју случајева (64%) не примењује уопште;
- Мере заштите податка о личности које се користе су: чување података на посебном рачунару; систем лозинки; приступ има само овлашћено лице; папирне збирке података у закључаним просторијама, дежурно лице и видео надзор.

КРАТАК ПРЕГЛЕД ДАТИХ ПРЕПОРУКА

1. Потребно је **да се што раније све јединице локалне самоуправе повежу на јединствену информмационо-комуникациону мрежу органа јавне управе (ЈИК мрежу)** како би били обухваћени заштитом коју у складу са чланом 8. Закона о електронској управи пружа Канцеларија за ИТ и еУправу, као ЦЕРТ републичких органа.
2. **Канцеларија за ИТ и еУправу би требало да донесе смерницу са препорученим софтверима за локалне самоуправе**, будући да велики број локалних самоуправа користи застареле софтвере, системе и апликације, као и бесплатне верзије антивирус програма.
3. Неопходно је систематизацијом радних места предвидети да **најмање један запослени у локалној самоуправи обавља послове администратора система и администратора мреже.**
4. Како би Канцеларија за ИТ и еУправу била у могућности да адекватно штити мрежу органа јавне управе, потребно је **успоставити јасне процедуре за управљање, коришћење и заштиту ЈИК мреже, мрежни оперативни центар (енг. *Network Operation Center - NOC*), оперативан ЦЕРТ државних органа и тим за одговор на инциденте (енг. *Incident Response Team*) и за аналитику за учење на грешкама** у складу са извештајима ИКТ система од посебног значаја.
5. **Канцеларија за ИТ и еУправу** у сарадњи са инспекцијом за информациону безбедност би требало да прати спровођење обавеза из Закона о информационој безбедности од стране органа јавне управе и **изда смернице за интерне процедуре и стандарде** како **за превенцију**, тако **и за поступање по претњама и инцидентима** којима буду изложени, а посебно за опоравак у случају катастрофа и обезбеђивање континуитета пословања. На основу утврђеног стања и праћења примене ових смерница **потребно је да се обавезне процедуре за органе јавне управе стриктније пропишу** допуном Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја.
6. Предлаже се и **успостављање мреже систем администратора** (запослених / задужених за ИТ) **локалних самоуправа** (уз подршку Националног ЦЕРТ-а или ЦЕРТ-а републичких органа), који би били у прилици **да на заједничкој платформи размењују информације, знања и искуства и једни другима обављају редовну екстерну проверу информационих система**.
7. Како је код инцидената и успешног реаговања најважније време, потребно је **успоставити механизам за једноставно обавештавање и координацију Националног ЦЕРТ-а, ЦЕРТ-а републичких органа, МУП-а, Повереника за информације од јавног значаја и заштиту података о личности и Тужилаштва за високотехнолошки криминал**. Потребно је изменом Закона о информационој безбедности прописати да сви (па и локалне самоуправе) инциденте пријављују преко јединствене платформе, преко које се директно обавештавају сви претходно наведени органи када је прописано законом, а како би у најкраћем року била обезбеђена адекватна подршка и како би се спречила штета већих размера. Како би ово било могуће, неопходно је прописати Законом о информационој безбедности обавезу свих органа јавне управе да инцидент пријаве свом ЦЕРТ-у, односно Канцеларији за ИТ и еУправу.

NALED
Savez za e-upravu
E-Government Alliance

ДЕТАЉНО ИСТРАЖИВАЊЕ

УВОД

У јануару 2020, НАЛЕД је спровео анкету о информационим системима локалних самоуправа. Подаци су прикупљани у циљу израде нове анализе о информационим системима и поређења са претходном, како би се дошло до сазнања о стању информационих система, као и да би се уочио евентуални напредак у односу на 2018. годину. Крајњи циљ јесте јачање капацитета локалних самоуправа и јачање информационе безбедности.

Ова анализа се израђује у оквиру пројекта *Јачање капацитета локалних самоуправа у примени регулативе у области информационе безбедности*, који је у другој половини 2019. године спроведен у сарадњи са РАТЕЛ-ом, а уз подршку Министарства трговине, туризма и телекомуникација и Канцеларије за информационе технологије и електронску управу.

Извештај се састоји из три дела. У првом делу даје се преглед основних и најважнијих резултата анализе. У другом делу приказујемо резултате истравање спроведеног почетком 2020. године, које се односи на 2019. годину. Трећи део приказује компаративну анализу резулатата истраживања за 2019. годину у односу на 2018.

МЕТОДОЛОГИЈА

Током јануара 2020. године организовано је прикупљање података од локалних самоуправа на основу упитника развијеног у претходној фази истраживања (2018. године) у циљу поређења добијених резултата. Упитник је послат електронским путем свим локалним самоуправама у Србији – општинама, градовима и градским општинама Града Београда. Локалне самоуправе су имале рок од 10 радних дана за електронско попуњавање упитника.

Укупно 69 локалних самоуправа доставило је податке о стању информационих система, од чега је 50 општина, 15 градова и 4 градске општине.

Резултати су пописани и креирана је база података у *excel* формату која је коришћена за обраду података. Извршена је дескриптивна обрада података, као и компарација резултата са прошлогодишњим.

Карактеристике локалних самоуправа у узорку

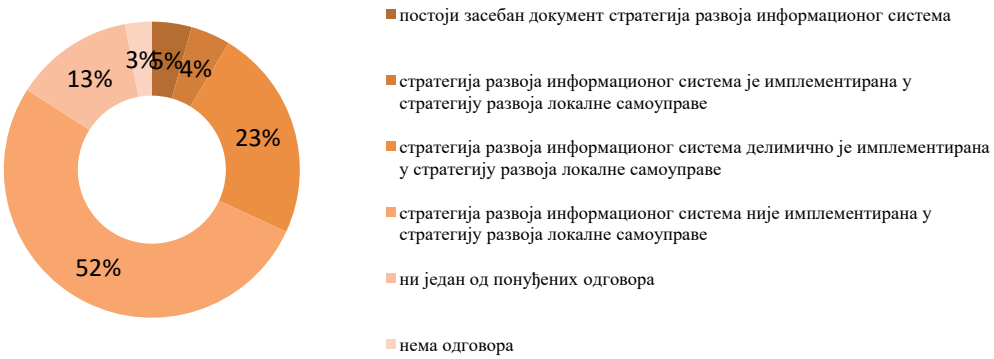
- На основу анализираног узорка, просечан број запослених у општинама је 76, у градским општинама 146, а у градовима 272 (не рачунајући Град Београд и Град Нови Сад који имају преко 1.000 запослених). Лица су запослена на основу уговора о раду, уговора о делу, уговора о привремено-повременим пословима и уговора о обављању стручне праксе;
- У просеку, 1 лице је ангажовано на сваких 62 запослена у локалној самоуправи;
- Надлежност за управљање информационим системима је на нивоу одељења (30 локалних самоуправа), одсека (9 локалних самоуправа), служби (7 локалних самоуправа) или група (2 локалне самоуправе). Чак 18 локалних самоуправа нема посебну организациону јединицу која се бави одржавањем информационог система, док неке имају уговоре са екстерним компанијама;
- 18% локалних самоуправа није доставило податке о буџетима за ИТ за текућу годину или немају исказану посебну ставку за ИТ у оквиру укупног буџета. Према достављеним подацима, општине ће у 2020. години у просеку издвојити 2.977.667 дин, градови 25.605.089 дин, а испитане градске општине 7.358.250 дин за сервис рачунара и опреме, одржавање постојећих и набавку нових софтвера, нове опреме и осталих трошкова за одржавање система и мреже.

ДЕТАЉНИ РЕЗУЛТАТИ ИСТРАЖИВАЊА ЗА 2019. ГОДИНУ

1. **Да ли имате израђен Акт о информационој безбедности и да ли се стриктно примењује?**

   Свега 19% (13 од 69) локалних самоуправа је навело да имају Акт и да се стриктно примењује. Са друге стране, 47% (32 од 69) локалних самоуправа има израђен Акт о информационој безбедности, али нема контролне механизме примене, односно Акт се не примењује стриктно, 22% (15 од 69) је у фази израде Акта, док га 9% (6 од 69) нема уопште. Већина локалних самоуправа је нагласила да планира доношење Акта, његову ревизију или пуну имплементацију у 2020. години.

2. **У којој мери је стратегијом развоја локалне самоуправе обухваћен информациони систем?**



   У већини анкетираних локалних самоуправа, чак 52% (36 од 69) стратегија развоја информационог система није обухваћена стратегијом развоја локалне самоуправе и не зна се у ком обиму подржава развој пословних процеса. Свега 4% (3 од 69) локалних самоуправа има стратегију информационог система као део стратегије развоја локалне самоуправе, док је 23% (16 од 69) стратегију имплементирало делимично. Такође, 4% (3 од 69) локалних самоуправа стратегију развоја информационих технологија има као засебан документ.

3. **У којој мери је реализована стратегија развоја информационог система локалне самоуправе?**

   Већина локалних самоуправа је на ово питање дала одговор „ниједан од понуђених одговора“, напомињући да оваква стратегија не постоји или да није никада имплементирана. Од 31 локалне самоуправе која има или је имала стратерију развоја информационог система, свега 29% (9 од 31) је навело да је стратегија реализована преко 80%, 29% (9 од 31) да је реализована преко 50%, док је у 16% (5 од 31) локалних самоуправа стратегија реализована испод 50%. Додатно, у 13% (4 од 31) локалних самоуправа се од израде овакве стратегије одустало.

4. Које промене су предвиђене у оквиру планова развоја током 2020. године?

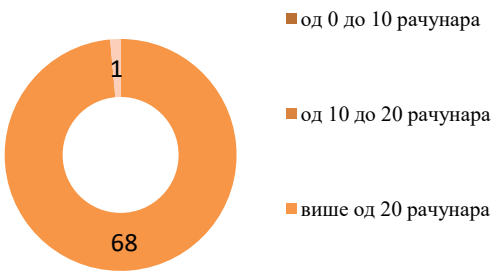
Како је приказано у табели, готово половина локалних самоуправа (34 од 69) планира да у току 2020. године промени серверску инфраструктуру, 36% (25 од 69) систем информационе безбедности, 35% (24 од 69) комуникациону опрему, док 27.5% (19 од 69) планира да мења главну пословну апликацију или њен део. Више од половине локалних самоуправа навело је да планира симултане промене више сегмената информаконог система током ове године. Са друге стране, 22% (15 од 69) анкетираних локалних самоуправа не планира никакве промене.

Врста промене	Број ЈЛС
Серверска инфраструктура	34
Систем информационе безбедности	25
Комуникациона опрема	24
Главна пословна апликација или њен део	19
Нису предвиђене промене	15
Систем физичке безбедности	12
Дата центар	7
Нема одговора	2
Ниједан од понуђених одговора	1

5. На који начин сте повезани на интернет и да ли су подаци угрожени?

62% (43 од 69) локалних самоуправа наводи да су подаци којима располажу угрожени јер имају приступ интернету (повезаност углавном оптичким каблом). Тек 22% (15 od 69) локалних самоуправа сматра да им подаци нису угрожени јер их чувају на посебним рачунарима који немају излаз на интернет или имају антивирус софтвер и *firewall*-ове, док неке наводе да имају интернету путем *proxy* сервера који филтрира дозвољене веб странице када се дефинишу.

6. Колико расположивих рачунара има у ЈЛС?



Број расположивих рачунара у већини случајева кореспондира са бројем запослених у локалној самоуправи или га незнатно надмашује.

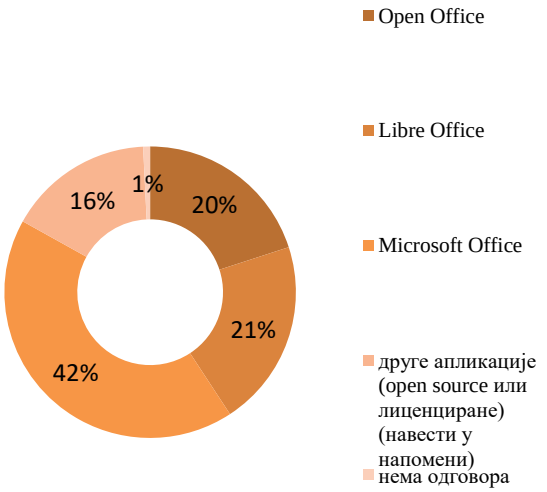
Од додатне мрежне опреме ЈЛС су наводиле да поседују *switch*-еве и рутере, док су доминантни произвођачи *Microtic, TP Link* и *Cisco.*

7. Које оперативне системе користите?

Већина локалних самоуправа, њих 86% (59 од 69) користи више оперативних система. Процентуално се највише користе *Windows 10* (98%) и *Windows 7* (97%). Један део користи и *Windows XP* (62%), али не као примарни оперативни систем већ један од и то у мањем броју случајева. Најмање се користи *Linux* односно *Unix* (32%). 85% локалних самоуправа користи више оперативних система симултано.

Од осталих оперативних система користе се и *Windows server* 2008, *Windows server* 2012, *Windows server* 2016.

8. Наведите апликације које користите као *open source* и лиценциране апликације?



Апликација која се највише користи је *Microsoft Office*. Мањи број апликација је лиценциран и такође зависи од броја рачунара на којима се користи, те варира од две лиценце до 295 лиценци. Неке користе и нелиценцирану верзију. Приближно у истој мери се користе *Libre Office* и *Open Office*.

Један део локалних самоуправа користи више различитих апликација истовремено. Друге апликације најчешће у употреби су *AutoCAD, Paragraf Lex, еЗУП, Буџетски саветник, Хермес, Пупин ЛПА, Adobe Reader* и друге.

9. На који начин се води евиденција хардверских и софтверских компоненти у локалној самоуправи?

Локалне самоуправе евиденцију хардверских и софтверских компоненти убедљиво највише воде уз помоћ књиговодствених евиденција, односно на основу евиденције годишњег пописа. Поред тога, у 35% (16+8 од 69) локалних самоуправа користе интерне помоћне табеле, или посебна апликативна решења/софтвере како би водиле евиденцију о хардверима и софтверским компонентама које поседују. У 9% (6 од 69) локалних самоуправа не води се евиденција хардверских и софтверских компоненти ни у каквом облику. Неколико ЈЛС користи више начина евиденције хардвера и софтвера.

Евиденција харверских и софтверских компоненти	Број ЈЛС
Књиговодствене евиденције, односно евиденције годишњег пописа	52
Помоћне табеле без детаљно описаних међузависности	16
Апликативно решење у коме се воде ажурне евиденције хардверских и софтверских компоненти и њихове међузависности	8
Не води се евиденција хардверских и софтверских компоненти	6
Ниједан од понуђених одговора	2

10. **Да ли је класификација, обележавање и поступање са информационим добрима према степену осетљивости и критичности прописана унутрашњим актом?=**

У 45% (31 од 69) локалних самоуправа класификација, обележавање и поступање са информационим добрима према степену осетљивости и критичности није прописана унутрашњим актом. У 16% (11 од 69) локалних самоуправа јесте прописана унутрашњим актом и доследно се примењује, у 13% (9 од 69) се не примењује доследно, док је у 14% (10 од 69) израда акта у току.

11. **Да ли користите *WiFi* и *Bluetooth* технологију и да ли су те врсте конекција заштићене?**

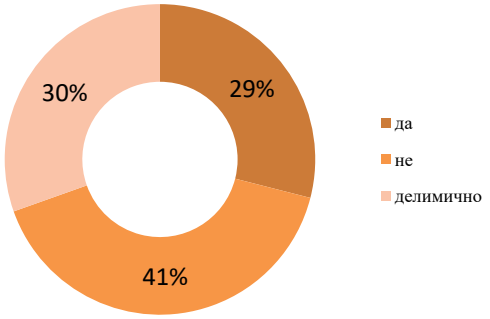
Чак 83% (57 од 69) локалних самоуправа користи *WiFi* и *Bluetooth* технологију која је заштићена. Локалне самоуправе које су додале и напомену уз ово питање нагласиле су да је *WiFi* одвојен од локалне мреже која се користи за повезивање запослених на интернет (5 од 5 локалних самоуправа). Међутим, 6% (4 од 69) локалних самоуправа наводи да користе *WiFi* и *Bluetooth* али нису заштићене. Такође, 12% ЛС (8 од 69) навело је да их не користи уопште.

12. **Каква је организациона структура ИТ одељења, број запослених и њихов профил (знање, вештине и образовање)?**

Чак 97% (67 од 69) локалних самоуправа има од 0 до 10 запослених у ИТ сектору. Тек 3% (2 од 69) локалних самоуправа имају од 10 до 20 запослених (Град Крагујевац и Град Зрењанин).

У већини локалних самоуправа ИТ кадар је високо образован, док неки имају завршене више школе и бројне сертификате. Неколико локалних самоуправа је навело да користи услуге екстерне фирме која обавља послове у вези са одржавањем информационог система.

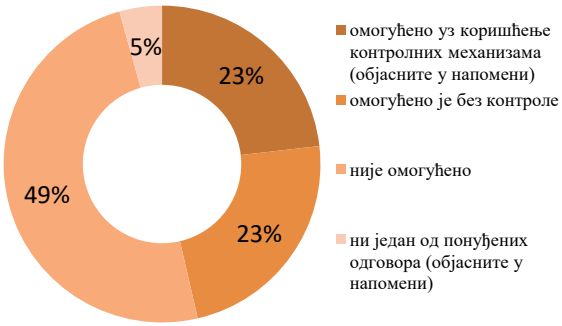
13. **Да ли запослени имају ограничен приступ садржајима на интернету?**



На основу података добијених упитником у 40% (28 од 69) локалних самоуправа запослени имају неограничен приступ садржају на интернету. У 29% (20 од 69) приступ је ограничен, док је у 31% (21 од 69) ограничен делимично.

Код локалних самоуправа које ограничавају приступ садржаја на интернету ограничава се и приступ друштвеним мрежама, веб страницама са непримереним садржајем, игрицама, док неке наводе да одређени запослени имају неограничен приступ садржајима на интернету због природе посла који обављају. Приступ се ограничава *blacklist*-овањем страница, помоћу *firewall*-а, веб филтрирањем, контролом логова итд.

14. Да ли запослени могу користити сопствене уређаје за приступ информационом систему локалне самоуправе?



Упитником је утврђено да 49% (34 од 69) локалних самоуправа не дозвољава коришћење сопствених уређаја запослених за приступ информационом систему. Подједнак број ЛС омогућава приступ без контроле и уз коришћење контролних механизама.

ЛС које користе контролне механизме приликом омогућавања коришћења сопствених уређаја запослених за приступ информационом систему наводе да се сопствени уређаји користе за приступ бежичној мрежи, али не и локалној пословној мрежи. Неке омогућавају приступ уз коришћење посебне лозинке или сертификационе картице, али се у већини овакав приступ третира као изузетак, а не правило.

15. На који начин се управља корисничким правима приступа информационом систему (радне станице, апликације, сервиси, мрежни уређаји)?

Корисничким правима приступа информационом систему се у 45% (31 од 69) локалних самоуправа управља посебно у зависности од апликације односно система у коме се приступа, док у 30% (21 од 69) се управљање врши централизовано за све апликације које се користе у ЛС.

16% локалних самоуправа (11 од 69) навело је да управља приступом системима делимично – односно за неке системе и апликације постоји контрола приступа, за неке не. У 7% (5 од 69) локалних самоуправа се уопште и не управља приступом.

Централизовано се најчешће управља путем активног директоријума или доменске мреже. Посебно се управља путем различитих програма или су корисничким налозима одређена права приступа. Делимично се управља када је део обухваћен доменском мрежом, а део није, или када само део запослени користи одређени софтвер, а други део не.

16. На који начин се приликом употребе информационог система (искључујући удаљени приступ) проверава идентитет запослених?

70% ЛС приликом употребе информационог система идентитет запослених проверава употребом корисничког имена и лозинке. Свега 20% ЛС користи паметну картицу са сертификатом, а само 9% користи токен.

Додатно, 26% (18 од 69) локалних самоуправа је нагласило да користе више фактора симултано, с тим што се картице са сертификатом користе за логовање на портале као што су Портал еУправа, еПорези и слично, а корисничко име и лозинка за интерне системе.

17. На који начин се приликом удаљеног приступа информационом систему проверава идентитет запослених?

У већини локалних самоуправа се за удаљени приступ информационом систему користе корисничко име и лозинка уз ВПН приступ. Подједнак број локалних самоуправа користи паметну картицу са сертификатом или нема могућност удаљеног приступа или такав приступ третира као изузетак. Неке користе и ОТП једнократну лозинку у изузетним случајевима, нпр. када одржавалац неког софтверског решења има потребу за неком интервенцијом. Такође, неке локалне самоуправе користе и ТАН таблице.

На основу добијених података 19% (13 од 69) локалних самоуправа комбинује више различитих решења за омогућавање удаљеног приступа информационом систему.

18. Да ли запослени на својим рачунарима користе лозинке приликом пријављивања на систем и колико их често мењају?

Готово је подједнак број локалних самоуправа чији запослени користе лозинке приликом пријављивања на систем и мењају их (49%) и оних чији запослени користе лозинке али их не мењају (50%). Само једна локална самоуправа је пријавила да њени запослени не користе лозинке приликом пријављивања на систем. Учесталост промене лозинке зависи од локалне самоуправе до локалне самоуправе. Неке немају података о томе колико често запослени мењају лозинке, док се у неким то ради једном месечно, квартално, једном у шест месеци или на годину дана. Негде лозинке мења и сам администратор.

19. Да ли су радне станице укључене у домен или се запослени пријављују искључиво локално на рачунар?

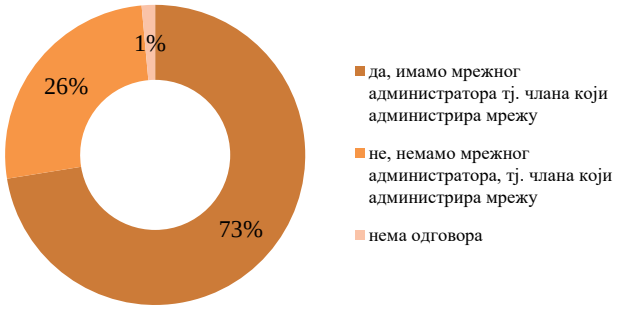
У већини локалних самоуправа (њих 54%, односно 37 од 69) радне станице су укључене у домен.

Међутим, у не тако занемарљивом броју од 30 локалних самоуправа (43%) запослени се пријављују локално на рачунар. Ни у једној локалној самоуправи запослени не раде без пријављивања, било на домен или локално на рачунар.

20. На који начин се спречавања неконтролисани одлив информација из ЈЛС?

66% локалних самоуправа не контролише одлив информација из локалне самоуправе. Са друге стране, 11% ЛС контролише приступ јавним сервисима за размену и чување докумената, 9% електронску пошту, 6% преносиве меморијске уређаје, а 5% приступ јавним сервисима електронске поште. Додатно, неколико локалних самоуправа је навело да је у току набавка одговарајућег софтвера у ове сврхе.

21. Да ли организациона структура одељења подразумева члана чији опис послова обухвата администрирање мреже (мониторинг, конфигурацију *firewall*-а, *IDS/IPS* решења, мрежне опреме)?



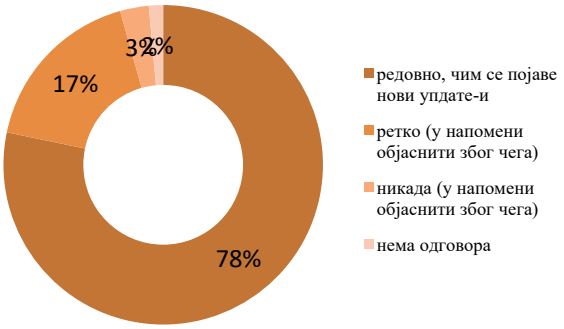
50 локалних самоуправа, односно 72%, је одговорило да имају мрежног администратора, док је остатак од 26% (18 од 69) навело да немају мрежног администратора.

Међу онима које су одговориле да имају мрежног администратора неколико је оних које су наводиле да је у питању екстерна ангажована компанија. Оне које немају мрежног адмнистратора напомињу да не постоји опредељено место за ту позицију, већ све послове у вези са одржавањем мреже обавља лице које се бави и другим пословима везаним за информационе технологије.

22. Ко обавља конфигурисање и одржавање сигурносних алата, апликација и инфраструктуре?

67% ЛС (46 од 69) има задуженог члана за конфигурисање и одржавање сигурносних алата, апликација и инфраструктуре, док 32% ЛС (22 од 69) немају. Поново, већи део оних које су одговориле да имају лице које се бави овим пословима је навело да су у питању *outsource*-ване услуге или да ове послове обавља лице које се бави и одржавањем система и мреже и обавља друге послове из ИТ сектора.

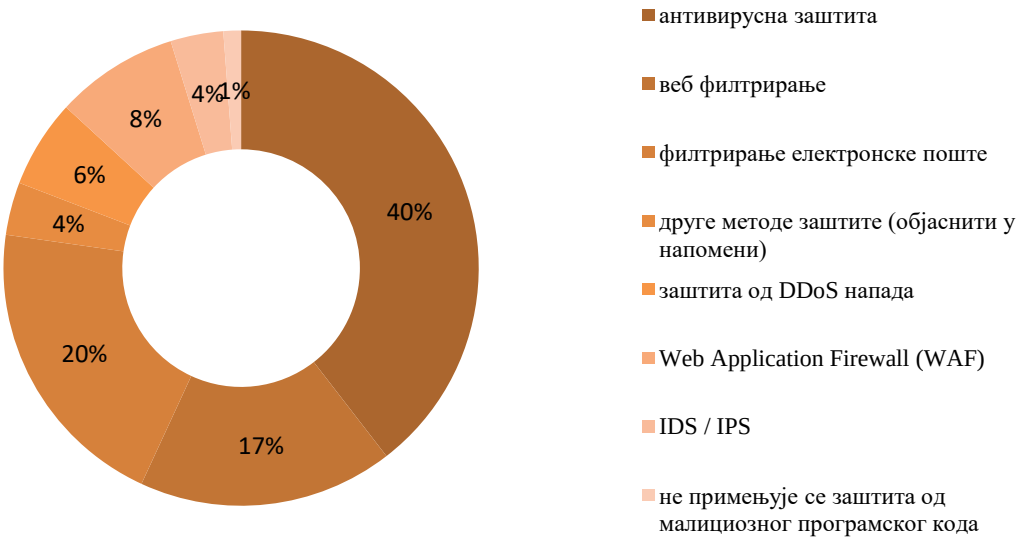
23. Колико често вршите *update* система?



Већина локалних самоуправа врши *update* система чим се појаве нови *update*-ови. 17% (12 од 69) локалних самоуправа то чини ретко, а само 3% (2 од 69) никада. Као разлог за ретко *update*-овање система наводи се застарелост програма и апликација у употреби где „више проблема настане након *update*-овања него без“ и условљеност природом посла који се обавља.

24. Шта се користи за заштиту информационог система од малициозног програмског кода?

59% (41 од 69) локалних самоуправа користи више начина заштите од малициозних програмских кодова симултано. Процентуално се највише користи антивирус, те филтрирање електронске поште, а затим веб филтрирање. Остале методе које су у примени су и заштита од *DDos* напада, *WAF (Web Application Firewall)*, и *IDS/IPS*.
3% (2 од 69) локалних самоуправа не примењују никакав облик заштите.



25. Да ли ЈЛС врши *backup* података, база и система од примарне важности као додатан вид заштите у случају напада енкрипцијом (*ransomware*), малициозних напада, физичке штете, заштите од губитка података и сл?

78% (54 od 69) локалних самоуправа имају независне резервне копије података, база и система. Са друге стране, 19% (13 од 69) наводи да уопште не ради резервне копије, док 3% ЛС (2 од 69) наводи да их ради делимично, односно да се *backup* ради за неке податке, базе и системе, а за неке не.

26. На који начин се врши управљање системским и оперативним записима?

У приближно једнакој размери се логовима управља посебно (38%) или се не управља уопште (33%).

У нешто мањој мери се записима управља делимично, док се у 9% локалних самоуправа записима не управља уопште.

27. Да ли организујете обуке и подизање свести о информационој безбедности?

77% (53 од 69) локалних самоуправа су нагласиле да организују обуке за подизање свести о информационој безбедности, док 23% (16 од 69), односно готово свака четврта, овакве обуке не организује. Оне које су навеле да обуке организују под тиме подразумевају и одласке на семинаре НАЛЕД-а или других организатора. Неке наводе да се обуке организују по потреби или врло ретко, док је неколико локалних самоуправа одговорило да под обуком подразумева и давање обавештења запосленима од стране ИТ лица.

28. Које *firewall*-ове и *IDS/IPS* уређаје користите?

43% (30 од 69) локалних самоуправа има *firewall* и *IDS/UPS* уређаје, док је 35% (24 од 69) ЛС навело да не их користе. 16% ЛС (11 од 69) је навело да их има делимично, односно да их на неким рачунарима користе, а на неким не. Најзаступљенији су *Microtic, Cisco, Microsoft*, као и *Sophos*.

29. Шта користите од антивирус софтвера и на који начин штитите рачунарску мрежу?

93% испитаних локалних самоуправа има антивирус софтвер, док 3% локалних самоуправа нема антивирусе. Од антивирус софтвера најчешће се користе: *Eset Endpoint, Kaspersky, Avast, Sophos Endpoint, Microsoft Security Essentials, Windows Defender*, као и друге доступне и бесплатне верзије софтвера.

30. Да ли постоје делови система који се могу окарактерисати као крхки?

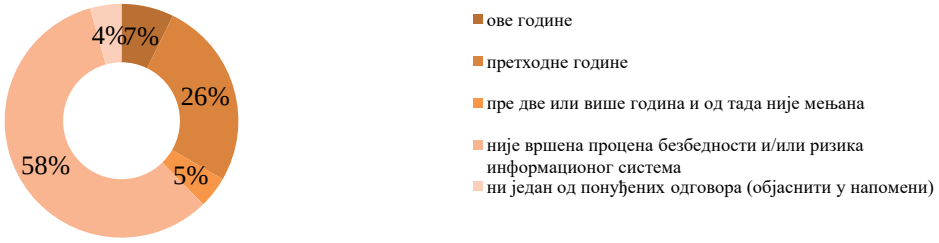
74% локалних самоуправа сматра да имају крхке делове система, са тендендијама да падну. 26% сматра да су им системи стабилни.
Већина локалних самоуправа је истакла проблем коришћења старијих оперативних система као главни фактор слабости система у употреби, у првом реду *Windows XP*-а.

31. Да ли користите и чије консултантске услуге у домену информационе безбедности?

78% (54 од 69) локалних самоуправа користи услуге екстерних компанија у домену информационе безбедности. 19% (13 од 69) локалних самоуправа не користи консултантске услуге када је реч о информационој безбедности већ све обавља самостално.

32. Последња процена безбедности и/или ризика информационог система:

Већина локалних самоуправа (58%) није вршила никакву процену безбедности и/или ризика информационих система. 26% (18 од 69) локалних самоуоправа је такву процену извршило прошле године, 7% (5 од 69) ове године, а 4% (3 од 69) пре две или више година. Неколико локалних самоуправа сматра да такве процене нису неопходне, с обзиром да се стално врши *upgrade* система, прати антивирус софтвер, скенира локална мрежа итд.



33. Када је вршена последња процена ризика информационог система?

61% (42 од 69) локалних самоуправа није никада вршило процену ризика информационог система. 22% (15 од 69) је нагласило да је процена ризика вршена прошле године, 7% (5 ЛС) да је вршена ове године (под овим се мислило на 2019-у годину), а 4% (3 ЛС) пре две или више година.

И у овом као и у претходном питању, под проценама ризика које су вршене прошле године, мисли се на попуњавање ове анкете, док су неке навеле и пен тестирање које је извршила компанија *SAGA* у новембру 2018.

34. Да ли постоји усвојен план опоравка у случају катастрофа?

Ниједна од испитаних локалних самоуправа није усвојила и тестирала план опоравка у случају катастрофа у последњих годину дана. Иако је већина ЛС изабрала „ниједан од понуђених одговора“ нагласивши да немају такав план, ипак постоје ЛС које имају овакве планове.

Наиме, у 23 локалне самоуправе у току је израда плана континуитета пословања, 3 су одговориле да су усвојиле такав план и да га никада нису тестирале, а још 3 да су га усвојиле, али га нису тестирале у последњих годину дана.

35. Када се креирају резервне копије података?

Процентуално се у највећем броју локалних самоуправа резервне копије података креирају дневно (67%), те по потреби (42%), затим недељно (39%), а најређи случај је да се резервне копије креирају месечно (25%). 43% локалних самоуправа је на ово питање дало више од два одговора, у зависности о каквим подацима је реч. Једна локална самоуправа је напоменула да резервне копије података креира на полугодишњем и годишњем нивоу.

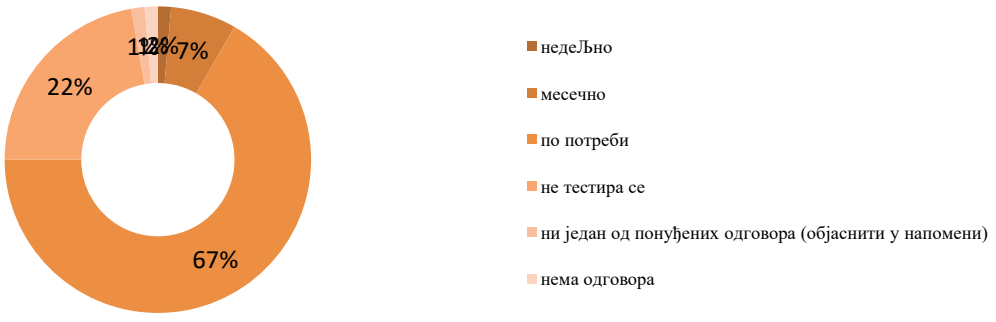
36. Које типове резервних копија података локалне самоуправе праве?

72% локалних самоуправа прави комплетну резервну копију података. 25% локалних самоуправа креира инкременталне копије, а 20% диференцијалне. 22% (15 од 69) локалних самоуправа је нагласило да креира више врста резервних копија података, у зависности од система које користе.

37. Где се чувају резервне копије података?

81% локалних самоуправа чува резервне копије података на локацији примарног рачунарског центра, 20% локалних самоуправа резервне копије података чува на посебној удаљеној локацији, док 13% чува копије на локацији резервног рачунарског центра. 7% локалних самоуправа резервне копије чува на екстерним хард дисковима или другде. 16% локалних самоуправа је дало два или више одговора на ово питање.

38. Када се тестира опоравак из резервних копија података?



67% локалних самоуправа тестира опоравак из резервних копија података по потреби. 22% локалних самоуправа уопште не тестира опоравак из резервних копија података. Мањи број тестира месечно, а само једна недељно.

39. Да ли је у последњих годину дана локална самоуправа је била изложена прекидима у раду?

Највећи број ЛС, чак 74% (51 од 69) је било изложено прекидима у раду услед нестанка струје. Остали фактори који су доприносили прекидима у раду су и телекомуникациони линкови, мрежна инфраструктура, те главна пословна апликација, мада већина наводи да су сви ови прекиди углавном последица прекида у електричном напајању, редовног одржавања, напада вируса или пада система услед застарелости сервера, рачунара или програма у употреби. 41% (28 ОД 69) локалних самоуправа је на више начина било изложено прекидима у раду у прошлој години, док 7% ЛС наглашава да није било никаквих прекида у раду у току прошле године.

40. Да ли постоји увојен и тестиран план континуитета пословања?

48% (33 од 69) локалних самоуправа је навело да нема усвојен план континуитета пословања. Такође, 35%(24 од 69) локалних самоуправа навело је да је израда плана континуитета пословања је у току. Свега 8% (6 од 69) ЛС је навело да су план усвојиле, али га никада нису тестирале.

41. Који су најчешћи напади на информациони систем и колико често се такви напади дешавају?

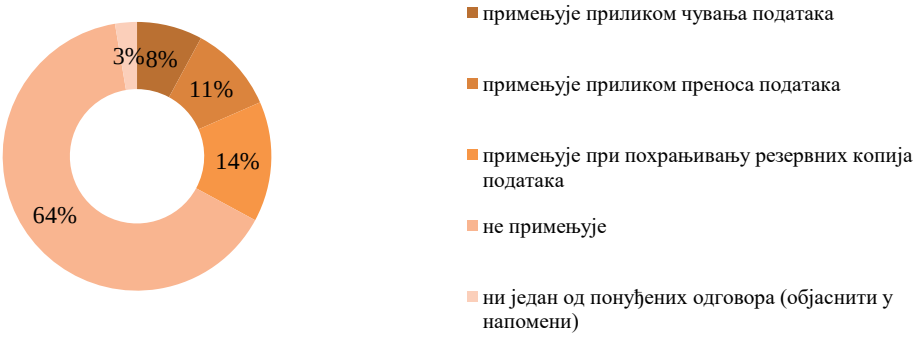
46% (32 од 69) локалних самоуправа забележиле су неки вид напада на информациони систем. 42% (29 од 69) тврди да није забележило ниједан вид напада на системе. Додано, 12% (8 од 69) локалних самоуправа не зна да ли је било изложено нападима.

Како наводе ЛС које су претрпеле нападе, најчешћи су напади на електронску пошту у виду спам мејлова, помоћу малициозних софтвера, потом напади на веб презентације, на рутер и *wifi* мрежу итд.

42. Да ли се примењује енкрипција осетљивих података?

Према резулатима анкете, енкрипција осетљивих података се у највећем броју случајева не примењује уопште. Чак 64% анкетираних локалних самоуправа ово наводи.

У 14% локалних самоуправа енкрипција осетљивих података се примењује при похрањивању резервних копија података, у 11% приликом преноса података, док се у 8% случајева примењује приликом чувања података.



43. Да ли постоје делови система који нису под директном контролом ЈЛС (физичка удаљеност или власничка контрола)?

У 58% (40 од 69) локалних самоуправа не постоје делови система који нису под директном контролом ЈЛС. Са друге стране, 40.5 (28 од 69) наводи да постоје делови система који се физички не налази у централи ЈЛС. Као пример се наводе месне канцеларије, односно физичку удаљеност радних станица смештених у њима.

44. Да ли се и који део посла са ИТ системима *outsource*-ује (које су то компаније и који је опис посла који обављају код вас)?

37 локалних самоуправа, односно 54% испитаних локалних самоуправа *outsource*-ује део посла из надлежности ИТ сектора. Углавном се *Outsource*-је одржавање система, сервисирање опреме, одржавање веб презентације, мрежне инфраструктуре итд. 29 локалних самоуправа односно 42%, не користи услуге екстерних ИТ компанија.

45. Да ли су базе података ЈЛС заштићене довољно јаким лозинкама?

Довољно јаким лозинкама се сматрају оне у којима се комбинују мала и велика слова, као и коришћење бројева и симбола и које су довољно дугачке.

Према резултатима анкете, 64% (44 од 69) локалних самоуправа сматра да су њихови системи и базе података заштићене довољно јаким лозинкама, док трећина анкетираних ЛС (23 од 69) сматра да нема довољно јаке лозинке. Оне које су нагласиле да немају довољно јаке лозинке напоменуле су да су администраторске лозинке јаке, али да немају увид у то колико су јаке корисничке лозинке, већ да они само могу дати препоруку какву је лозинку неопходно креирати.

46. Да ли је у последњих годину дана било околности које су захтевале активацију *BCP* и *DRP*?

Свега две локалне самоуправе (3% од анектираних) навеле су да су у последњих годину дана активирали *BCP* и/или *DRP* услед потербе да се замени хардвер или је било речи о хардверском кварy. Пар локалних самоуправа нагласило је да није имало озбиљније прекиде у раду, те да није било потребе за активацијом *BCP* и/или *DRP*. Преостале анкетиране локалне самоуправе или нису одговориле на ово питање, или су наводиле да не знају шта су скраћенице *BCP* и *DRP* (*Business Continuity Plan* и *Disaster Recovery Plan*).

47. На којој локацији се налази примарни рачунарски центар на коме се налазе главне пословне апликације?

87% ЈЛС је навело да се главне пословне апликације налазе у згради њихове локалне самоуправе, односно у сервер сали.

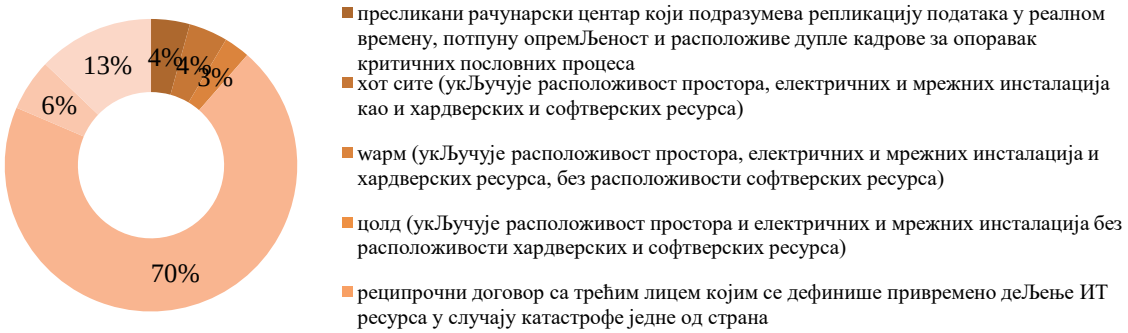
48. На којој локацији се налази резервног рачунарског центра на којој се налазе главне пословне апликације?

Већина локалних самоуправа које су учествовале у анкети није дала одговор на ово питање. Од оних које су одговориле у највећем броју случајева навођено је да немају резервни рачунарски центар или су наводиле исту локацију као за примарни рачунарски центар – сервер сала у згради општинске или градске управе.

49. На којој локацији се налазе остали рачунарски центари које локална самоуправа користи?

Већина локалних самоуправа је одговорила да не поседује резервни рачунарски центар. Неке су наводиле пример аликације ЛПА или Хермес информационог система.

50. Да ли имате резервни рачунарски центар?



Чак 70% локалних самоуправа нема резервни рачунарски центар. Остале нису одговориле на ово питање. Тек 4%, односно 3 локалне самоуправе од анкетираних 69 су одговориле да имају пресликани резервни рачунарски центар, 4% (3 ЛС) да имају *hot site* и 3% (2 ЛС) да имају *warm* што укупно чини свега 11% локалних самоуправа.15% локалних самоуправа је избегло одговор на ово питање.

51. Којим збиркама података о личности располаже Ваша ЈЛС и по ком правном основу?

Нажалост, мање од половине испитаних ЛС је одговорио на ово питање. 37% локалних самоуправа које су одговориле, навеле су да располажу различитим интерним евиденцијама запослених на основу њиховог пристанка, као и евиденцијама које се воде или су се водиле на основу посебних закона.

52. Које су мере заштите података о личности предузете у оквиру Ваше ЈЛС?

Најчешће мере заштите које су навођене у анкети су:

- чување података на посебном рачунару;
- систем лозинки и давање приступа само овлашћеном лицу;
- чување папирних збирке података у закључаним просторијама;
- ангажовање дежурног лица да чува збирке података у згради ЈЛС;
- видео надзор.

Неколико локалних самоуправа је навело да њихови акти не садрже такве податке који би изискивали посебну заштиту или да нема посебних мера заштите.

53. Ко су корисници ваших збирки података о личности и по ком основу?

Нажалост, већина локалних самоуправа није одговорила на ово питање или је дала неодређен одговор попут „подаци су доступни за јавност“, „подаци садрже прописани степен тајности и нису доступни другима“, „подаци су јавни осим у случајевима прописаним законом“. Као најчешћи корисници навођена су министарства и други државни органи, лица на која се подаци односе и овлашћени службеници.

КОМПАРАТИВНА АНАЛИЗА 2019. И 2018. ГОДИНЕ

НАПОМЕНЕ О УЗОРКУ

Податке о својим информационим системима у 2018. години су доставиле 63 локалне самоуправе, а у 2019. 69 локалних самоуправа. 49% узорка се поклапа, док је 51% узорка различито у односу на претходну анализу;

Број упитника	2018	2019	Преклапање узорка
	63	69	49%

Подаци о буџету, просечном броју запослених и организационом јединицама су приближно слични. У 2018. години буџет за ИТ за општине је износио око 2.200.000 дин, а 2019. 2.977.667 дин. Просечан број запослених у општинама је био 74, а у 2019. 76. ИТ је у 2018. години надлежност за управљање информационим системом је најчешће била на нивоу одељења (44%), што је случај и у 2019. години (43%);

У 2018. години, на основу испитаног узорка, 1 ИТ лице се ангажује на сваких 65 запослених. У 2019, тај однос је 1 наспрам 62.

Удео ИТ у односу на укупан број запослених	2018	2019
	1/65	1/62

КОМПАРАТИВНИ РЕЗУЛТАТИ

1. **Да ли имате израђен Акт о информационој безбедности и да ли се стриктно примењује?**

   У 2018. години свега 22% ЈЛС је имало израђен Акт о информационој безбедности и доследно следило његове процедуре. 32% их је имало, али нису постојали контролни механизми примене, а четвртина њих је навела да је у фази израде. 17% локалних самоуправа није имало израђен Акт.

   У 2019. години 19% локалних самоуправа је навело да доследно примењује Акт (3 процентна поена мање у односу на 2018. годину), чак 46% да га имају али немају контролне механизме (чак 14 процентних поена више у односу на 2018.), 22% је навело да је Акт и даље у фази израде, а 9% да га нема уопште (што је побољшање у односу на претходну годину);

Да ли постоји Акт о информационој безбедности и да ли се доследно примењује	2018	2019
Постоји и доследно се примењује	22%	19%
Постоји, али нема контролних механизама примене	32%	46%
Акт је у фази израде	25%	22%
Не постоји Акт о инф. безбедности	17%	9%

2. **У којој мери је стратегијом развоја локалне самоуправе обухваћен информациони систем?**

Када се погледа статус стратегије развоја информационог система у односу на стратегију развија локалне самоуправе резултати анализа су потпуно конзистентни. У половини локалних самоуправа стратегија развоја инфорамционог система није део стратегије развоја локалне самоуправе. У 9% ЛС постоји засебан документ, а у петини ЛС стратегија информационог система делимично је интегрисана у стратегију развоја локалне самоуправе (22% у 2018. односно 23% у 2019. години)

Да ли је стратегија развоја информационог система обухваћена стратегијом развоја локалне самоуправе	2018	2019
Није обухваћена	51%	52%
Обухваћена је или постоји засебан документ	9%	9%
Делимично је обухваћена	22%	23%

3. **У којој мери је реализована стратегија развоја информационог система локалне самоуправе?**

У 2018, 71% испитаних локалних самоуправа је изјавило да нема стратегију развоја информационог система, или да се од стратегије одустало, а у свега 6% локалних самоуправа је стратегија реализована више од 80%. У 2019, 61% општина и градова је навело да немају стратегију, или да су од њене израде одустали, 7% да имају стратегију али је реализована испод 50%, у 13% изнад 50%, док је 13% локалних самоуправа навело да имају стратегију и да је реализована изнад 80%; Дакле, иако је приближно исто учешће ЛС које имају статеријy развија информационог система, нешто већи број ЛС навео је да је реализовао стратегију више од 80% у односу на прошло истраживање. Охрабрује и чињеница да је мање учешће ЛС које немају стратегију, мада је овај проценат и даље веома висок.

У којој мери је реализована стратегија развоја информационог система	2018	2019
Не постоји стратегија или се од ње одустало	71%	61%
Стратегија је реализована више од 80%	6%	13%
Стратегија је реализована више од 50%	11%	13%
Стратегија је реализована мање од 50%	10%	7%

4. **Које промене су предвиђене у оквиру планова развоја током 2020. године?**

У 2018. биле су предвиђене промене серверске инфраструктуре, те комуникационе опреме, система информационе безбедности, главне пословне апликације и друге промене. У 2019. су промене серверске инфраструктуре поново на врху приоритета, затим следи систем информационе безбедности, па поново комуникациона опрема и главна пословна апликација. 2018. године 12 локалних самоуправа није планирало никакве промене, а у 2019. њих 15 што је приближно исто учешће у укупном броју ЛС;

5. **На који начин сте повезани на интернет и да ли су подаци угрожени?**

   2018-е 65% локалних самоуправа је сматрало да су им подаци угрожени, док у 20% ЈЛС то није био случај. 2019-е 62% сматра да су им подаци угрожени, а 22% локалних самоуправа да нису што не показује драстичне промене. У оба случаја наводи се приступ интернету, односно повезаност оптичким каблом на интернет и чување података на рачунарима који имају излаз на интернет као фактор ризика, док се код осталих подаци налазе на затвореним системима који немају излаз на интернет;

6. **Колико расположивих рачунара има у ЈЛС? Које оперативне системе користе у ЈЛС. Наведите апликације које користите као open source и лиценциране апликације?**

   У обе анализе се показало да већина локалних самоуправа има преко 20 рачунара, односно да број рачунара кореспондира са бројем запослених;

   Обе анализе су показале да већина локалних самоуправа користи више оперативних система симултано, док највећу заступљеност имају *Windows 7* и *Windows 10*;

   Од *open source* и лиценцираних апликација највише се користи *Microsoft Office*. Мањи број је лиценциран и такође зависи од броја рачунара на којима се користи. Приближно у истој мери се користе *Libre Office* и *Open Office*. Друге апликације најчешће у употреби су *AutoCAD, Paragraf Lex, е3УП, Буџетски саветник, Хермес, Пупин ЛПА, Adobe Reader* и друге;

7. **На који начин се води евиденција хардверских и софтверских компоненти у локалној самоуправи?**

   Обе анализе показале су да локалне самоуправе за евиденцију хардверских и софтверских компоненти најчешће су се користе књиговодствене евиденције, и у нешто мањој мери помоћне табеле;

8. **Да ли је класификација, обележавање и поступање са информационим добрима према степену осетљивости и критичности прописана унутрашњим актом?**

   2018. године у 40% локалних самоуправа класификација, обележавање и поступање са информационим добрима није било уређено интерним актом, док је у овој години учешће још веће (45%) што забрињава. Међутим, са друге стране део ЛС којима је поменуто питање било у фази израде у прошлом истраживању сада је уредило унутрашњим актима те се овај проценат повећао са 24% на 29%, док је проценат ЛС којима је израда акта у току смањен са 24% на 14%.

Да ли су класификација, обележавање и поступање са информационим добрима уређени унутрашњим актом	2018	2019
Уређени су унутрашњим актом који се доследно или делимично примењује	24%	29%
Нису уређени унутрашњим актом	40%	45%
Израда акта је у току	24%	14%

9. **Да ли користите *WiFi* и *Bluetooth* технологију и да ли су те врсте конекција заштићене?**

   75% локалних самоуправа је у 2018. изјавило да користи *WiFi* технологију и да сматра да је оваква врста конекције заштићена јер углавном није повезана са остатком *LAN* мреже. У овогодишњем истраживању чак 83% ЛС је изјавило исто чиме примећујемо тенденцију боље заштите конекције. За разлику од прошлогодишњих 9% ЛС које је изјавило да њихове конекције нису заштићене, сада је то изјавило 6% анкетираних ЛС.

10. **Каква је организациона структура ИТ одељења, број запослених и њихов профил (знање, вештине и образовање)?**

    Обе анализе су показале да у највећем броју локалних самоуправа ради од 0 до 10 запослених у ИТ-у, и то најчешће 1, 2 или 3 лица, с тим што неке сматрају запосленима и лица која ангажују на основу уговора са екстерном компанијом. У већини локалних самоуправа ради ИТ кадар са вишим или високим образовањем;

11. **Да ли запослени имају ограничен приступ садржајима на интернету?**

    Обе анализе показују конзистентне податке у вези са приступом запослених садржајима на интернету. Већина ЛС (57% у 2018. и 59% у 2019.) у потпуности или делимично ограничава приступ садржајима на интернету (углавном друштвеним мрежама, страницама са непримерним садржајима и сл.).

12. **Да ли запослени могу користити сопствене уређаје за приступ информационом систему локалне самоуправе?**

    Анализе показују да се стање није значајно променило ни по питању коришћења сопствених уређаја запослених за приступ интернету током рада. Наиме, око половине ЛС у потпуности не дозвољава приступ преко сопствених уређаја запослених, око четвртине (25% у 2018. и 23% у 2019.) дозвољава али уз коришћење лозинке, док остатак од око петине ЛС наводи да је у постпуности дозвољен приступ без икаквих ограничења;

Да ли се дозвољава коришћење сопствених уређаја запослених за приступ интернету	2018	2019
Није дозвољено	50%	49%
Дозвољено је без контроле	19%	23%
Дозвољено је уз коришћење лозинке	25%	23%

13. **На који начин се управља корисничким правима приступа информационом систему (радне станице, апликације, сервиси, мрежни уређаји)?**

Што се тиче управљања корисничким правима, стање се у појединим областима мења. Наиме, смањује се учешће ЈЛС које корисничким правима приступа информационим системима управљају посебно за сваки информациони систем – 52% је ово радило 2018. године док је исто учешће у 2019. години 46%. Други резултати – да се приступима управља централизовано или да се неким софтверима контролише приступ неким не – су углавном конзистентни.

На који начин се управља корисничким правима приступа информационом систему	2018	2019
Управља се централизовано	32%	30%
Управља се посебно	52%	46%
Управља се делимично	14%	16%

14. **На који начин се приликом употребе информационог система (искључујући удаљени приступ) проверава идентитет запослених?**

Проверавање идентитета запослених приликом употребе информационог система и у 2018. и у 2019. најчешће иде преко корисничког имена и лозинке, те картице са сертификатом, токеном и на други начин. Већина користи више фактора аутентификације;

За удаљени приступ се користе корисничко име и лозинка уз ВПН приступ. Подједнак број је одговорио да користи паметну картицу са сертификатом или *ниједан од понуђених одговора*, углавном наводећи да или не постоји могућност удаљеног приступа или се третира као изузетак. Неке користе и ОТП једнократну лозинку и ТАН таблице. 19% локалних самоуправа комбинује више различитих решења. У 2018-ој је највећи број такође користио корисничко име и лозинку, 19% њих још неки други фактор као што је паметна картица или токен (17). 25% локалних самоуправа није дозвољавало удаљени приступ информационом систему;

15. **Да ли запослени на својим рачунарима користе лозинке приликом пријављивања на систем и колико их често мењају?**

Претходна анализа је показала да ЈЛС углавном користе лозинке приликом пријављивања на систем, али да се оне ретко мењају (6 месеци до годину дана), док се у половини анкетираних локалних самоуправа лозинке не мењају уопште. Ове године је 50% ЈЛС такође напоменуло да лозинке не мења, али је друга половина одговорила да лозинке мења чешће, од једном месечно до једном у 3 месеца, док тек понека локална самоуправа наводи да се лозинке мењају ређе од тога;

16. **Да ли су радне станице укључене у домен или се запослени пријављују искључиво локално на рачунар?**

2018-е 48% радних станица није било у домену, а 52% јесте. 2019-е 54% испитаних локалних самоуправа наводи да су радне станице запослених у домену, а 43% да нису;

Да ли су радне станице укључене у домен	2018	2019
Радне станице су укључене у домен	52%	54%
Радне станице нису укључене у домен	48%	43%

17. На који начин се спречавања неконтролисани одлив информација из ЈЛС?

2018. године је 71% локалних самоуправа навело да не контролишу одлив информација из локалне самоуправе, а ове 66% што представља побољшање у домену сигурности података.Неке контролишу приступ јавним сервисима за размену и чување докумената, неке електронску пошту, преносиве меморијске уређаје или приступ јавним сервисима електронске поште, што је такође био у случај у 2019. години;

18. Да ли организациона структура одељења подразумева члана чији опис послова обухвата администрирање мреже (мониторинг, конфигурацију *firewall*-а, *IDS/IPS* решења, мрежне опреме)?

У 2018, као и у 2019. години, већина локалних самоуправа је пријавила да има мрежног администратора. Међу онима које су одговориле да имају мрежног администратора неколико је оних које су наводиле да је у питању екстерна ангажована компанија. Оне које немају мрежног администратора напомињу да не постоји опредељено место за ту позицију, већ све послове у вези са одржавањем мреже обавља лице које се бави и другим пословима везаним за ИТ;

Обе анализе су дале исти резулат када је реч о запосленом задуженом за одржавање сигурносних алата, апликација и инфраструктуре, али је овај запослени углавном задужен и за многе друге активности. Из истог разлога је део локалних самоуправа навео да нема запосленог који је задужен за обављање само овог дела посла. Локалне самоуправе такође ангажују и екстерне компаније;

19. Колико често вршите *update* система?

Обе анализе су показале да ЈЛС редовно врше *update* система, док неколицина то чини ретко (17% у 2018. години, 17% у 2019.);

20. Шта се користи за заштиту информационог система од малициозног програмског кода?

У 2018. години анализа је показала да све анкетиране локалне самоуправе користе антивирусну заштиту против малициозних програмских кодова, док је веома заступљено и филтрирање електронске поште и веб филтрирање. 2019. године су резултати нешто другачији, будући да 3% локалних самоуправа не примењују никакав облик заштите. 60% ЈЛС користи више начина симултано, од чега највише антивирус, па филтирирање електронске поште и веб филтрирање. Остале методе које су тренутно у употреби у неким ЈЛС су и заштита од *DDos* напада, *WAF (Web Application Firewall)*, и *IDS/IPS*;

Шта се користи за заштиту информационог система од малициозног програмског кода	2018	2019
Антивирус	100%	96%
Веб филтрирање	43%	42%
Филтрирање електронске поште	52%	49%
WAF (Web Application Firewall)	16%	20%
Заштита од *DDos* напада	16%	15%
IDS/IPS	8%	9%
Не примењује се никакав облик заштите	/	3%

21. Да ли ЈЛС врши *backup* података, база и система од примарне важности као додатан вид заштите у случају напада енкрипцијом (*ransomware*), малициозних напада, физичке штете, заштите од губитка података и сл?

2018-е 6% ЈЛС су пријавиле да немају независне резервне копије података, док тај проценат 2019. 3%. 2018. године је већина *backup* вршила делимично или у целости, док ове године 78% локалних самоуправа пријављују да имају независне резервне копије података, а 19% да *backup* раде за неке податке, базе и системе, а за неке не;

Да ли ЈЛС врши *backup* података	2018	2019
Да	70%	78%
Не	6%	3%
Делимично	24%	19%

22. На који начин се врши управљање системским и оперативним записима?

У 2018-ој се системским и оперативним записима најмање управљало централизовано, а већином се управљало посебно или делимично или се није управљало уопште. У 2019-ој приближно у једнаком броју се логовима управља посебно (39%) или се не управља уоппте (33%). 20% ЈЛС логовима управља делимично, а 9% централизовано.

Начин управљања логовима	2018	2019
Централизовано	5%	9%
Посебно	35%	39%
Делимично	29%	20%
Не управља се	32%	33%

23. Да ли организујете обуке и подизање свести о информационој безбедности?

2018. године је само 21% локалних самоуправа навело да се организује нека врста обуке запослених о информационој безбедности (укључујући и циркуларне мејлове који их обавештавају о могућим опасностима), а чак 76% је навело да овакве обуке не организује. Стање у овој години је потпун другачије с обзиром да чак 77% ЛС наводи да организују обуке и подизање свести о информационој безбедности (подразумевајући под тим и одласке на семинаре НАЛЕД-а или других

организатора или давање обавештења запосленима од стране ИТ лица), док је само 23% навело да овакве обуке не организује;

24. Које *firewall*-ове и *IDS/IPS* уређаје користите?

Слични су резултати обе анализе када је реч о инсталираним *firewall* и *IDS/UPS* уређајима (2018. године 35/63 их је имало, а ове године 30/69). Најшеће се користе *Microtic, Cisco, Microsoft*, као и *Sophos*;

Да ли имате инсталиран *firewall* или *IDS/UPS*	2018	2019
Да	55%	43%

25. Шта користите од антивирус софтвера и на који начин штитите рачунарску мрежу?

2018. године је 95% локалних самоуправа навело да користи антивирус софтвер, а ове године 93%. 2018. године су најзаступљенији били *Eset Endpoint, Avast, Kaspersky*, а ове *Eset Endpoint, Kaspersky, Avast, Sophos Endpoint, Microsoft Security Essentials, Windows Defender*. И 2018. и ове године локалне самоуправе су наводиле да користе бесплатне и доступне верзије софтвера;

26. Да ли постоје делови система који се могу окарактерисати као крхки?

И ове и 2018. године је сличан однос оних локалних самоуправа које сматрају да су им делови система крхки, са тенденцијом да падну (углавном због застарелости система у употреби) и оних које сматрају да су им системи стабилни – 2018. године 71% оних који сматрају да су им системи крхки и ове године 74%;

27. Да ли користите и чије консултантске услуге у домену информационе безбедности?

У 2018-ој години само 13% локалних самоуправа је навело да користи консултантске услуге у домену информационе безбедности, а 84% да не користе. Ове године је однос потпуно другачији, те 78% локалних самоуправа наводи да користе услуге екстерних компанија, а 19% да не користе чиме се показује да ЛС имају свест од томе да немају довољно капацитета за одржавање ИТ система и да се обраћају другима за помоћ.

28. Последња процена безбедности или ризика информационих ситема.

2018. године је чак 65% локалних самоуправа навело да ниједном није вршило процену безбедности или ризика информационог система, а чак и оне које су такве процене вршиле су то радиле ради формалности. Ове године такође 58% локалних самоуправа наводи да није вршило процену безбедности или ризика информационих система, чиме се види мало побољшање. Највећи део ЛС је процене безбедности својих система спроводило у ранијим годинама (2018. или 2017) а не у текућој (2019). Неколико ЛС сматра да овакве процене нису неопходне;

Када је извршена последња процена безбедности и/или ризика информационог система	2018	2019
Није вршена никада	65%	58%
Ове године	14%	7%
Прошле године	8%	26%
Пре две или више година	6%	4%

29. Да ли постоји усвојен план опоравка у случају катастрофа?

Прошлогоишње истраживање показује да скоро половина анкетираних ЈЛС није имала усвојен план активности у случају катастрофа, док га је само 10% имало. Ове године ниједна од испитаних локалних самоуправа није пријавила да је усвојила и тестирала у последњих годину дана план опоравка у случају катастрофа. Већина ЛС (55%) је изабрала „ниједан од понуђених одговора“ нагласивши да немају такав план. У 33% локалних самоуправа је израда у току, док је 4% одговорило да су усвојиле такав план и да га никада нису тестирале;

Да ли имате усвојен план опоравка у случају катастрофа	2018	2019
Немају усвојен план	48%	55%
Израда је у току	35%	33%
Усвојен је и тестиран у претходних годину дана	2% (1 локална самоуправа)	0
Усвојен, али није тестиран у претходних годину дана	5%	4%
Усвојен и није тестиран никада	3%	4%

30. Када се креирају резервне копије података? Које типове резерних копија се креирају? Где се чувају? Када се тестира рад резервних копија?

У 2018. години већина локалних самоуправа је нагласила да комбинује различите периоде за креирање резервних копија података, најчешће наводећи дневни ниво. У овој години је такође већина одговорила са два или више одговора и процентуално се поново највећи део резервних копија података креира на дневном нивоу, те по потреби, затим недељно, а тек онда месечно. Једна локална самоуправа је напоменула да резервне копије података креира на полугодишњем и годишњем нивоу;

Обе анализе су показале да локалне самоуправе најчешће креирају комплетну резервну података. Оно што је разлика у односу на претходну анализу јесте број локалних самоуправа које креирају комплетне копије података (2018. године 46%, ове 72%), инкременталне (2018. године 3, ове 23) и диференцијалне копије података (2018. године 2, ове године 19 локалних самоуправа);

Типови резервних копија података	2018	2019
Комплетна	46%	72%
Инкрементална	5%	33%
Диференцијална	3%	27%

У 2018. години 42% локалних самоуправа је пријавило да резервне копије података чува на локацији примарног рачунарског центра, 29% поред тога и на посебној удаљеној локацији, 3% на локацији резервног рачунарског центра, а 10% искључиво на посебној удаљеној локацији. У овој години чак 81% пријављује да чува резервне копије података на локацији примарног рачунарског центра, 20% на посебној удаљеној локацији, а 13% на локацији резервног рачунарског центра. 6% чува резервне копије података на екстерним хард дисковима или другде. 16% локалних самоуправа комбинује више локација;

Где се чувају резервне копије података	2018	2019
На локацији примарног рачунарског центра	42%	81%
На локацији резервног рачунарског центра	3%	13%
На посебној удаљеној локацији	10%	20%
На локацији примарног рачунарског центра и посебној локацији или другде	29%	16%

У 2018. години се опоравак из резервних копија података тестирао по потреби или се није тестирао уопште, а тек у 2 локалне самоуправе (4%) недељно или месечно. У 2019. години 70% локалних самоуправа опоравак из резервних копија података тестира по потреби, 23% не тестира уопште, мањи број месечно, а само једна локална самоуправа недељно;

31. Да ли је у последњих годину дана локална самоуправа је била изложена прекидима у раду?

Подаци за 2018-у показују да је највећи број ЈЛС имао одређене прекиде у раду, највише због прекида електричног напајања, па тек онда прекида мрежне инфраструктуре или телекомуникационих линкова. Навођени су и у мањој мери прекиди у главној пословној апликацији, хакерски напади и кварови на серверу, док 10 није пријавило никакве прекиде у раду. У 2019. је 41% локалних самоуправа на више начина било иложено прекидима у раду, с тим што у овој години прекиди рада нису били претежно узорковани прекидом у електричном напајању.. Остали фактори су такође били телекомуникациони линкови, мрежна инфраструктура и главна пословна апликација, мада већина наводи да су сви ови прекиди углавном последица прекида у електричном напајању, редовног одржавања, напада вируса или пада система услед застарелости сервера, рачунара или програма у употреби;

Узроци прекида у раду	2018	2019
Прекид у електричном напајању	73%	40%
Мрежна инфраструктура	35%	17%
Телекомуникациони линкови	33%	20%
Главна пословна апликација	13%	7%
Апликација за електронско банкарство	3%	4%
Остало	11%	12%

32. Да ли постоји усвојен план континуитета пословања информационих система?

У 2018. години је 60% локалних самоуправа навело да нема план континуитета пословања, 30% да је израда таквог плана у току, а само једна ЛГ (односно 2%) да има усвојен план, али да није тестиран у претходних годину дана. Ове године 48% ЛС наводи да нема план што је значајно смањење у односу на прошлу годину, у 35% ЛГ је израад плана у току, док је 9% ЛС навело да су план усвојиле, али га нису тестирале што је побољшање у односу на претходну годину;

33. Који су најчешћи напади на информациони систем и колико често се такви напади дешавају?

2018. године 38% локалних самоуправа навело је да су забележиле некакав вид напада на информационе системе путем електронске поште, али и да су бележиле *ransomware* нападе. 27 локалних самоуправа није пријавило никакве нападе, а 11 не зна да ли је било изложено нападима. Ове године су 32 локалне самоуправе забележиле неки вид напада на информациони систем, док 29 није. 8 локалних самоуправа не зна да ли је било изложено нападима. Најчешћи су напади на електронску пошту у виду спам мејлова, помоћу малициозних софтвера, потом напади на веб презентације, на рутер и *wifi* мрежу итд;

34. Да ли се примењује енкрипција осетљивих података?

У 2018. 71% анкетираних локалних самоуправа је пријавило да не примењује енкрипцију осетљивих података. Ове године тај проценат износи 64% што показује да су ЛС свесне да рукују осетљивим подацима које је потребно заштитити. 2018. године је 29% локалних самоуправа пријавило да примењује неку врсту енкрипције, најчешће приликом чувања података или похрањивања резервних копија, док ове године 14% локалних самоуправа је напоменуло да енкрипцију осетљивих података примењује при похрањивању резервних копија података, у 11% приликом преноса, а у 8% приликом чувања података;

35. Да ли постоје делови система који нису под директном контролом ЈЛС (физичка удаљеност или власничка контрола)?

У 2018-ој чак 66% локалних самоуправа навело је да немају делове система који нису под директном контролом локалне самоуправе, док је трећина навела да има, реферишући на локалне месне заједнице, систем ЛПА итд. У овогодишњем истраживању, нешто је мање учешће ЛС које све своје системе имају под директном контролом ЈЛС. 58% локалних самоуправа има цео систем под директном контролом ЈЛС, док 41% нема и наводи као пример месне канцеларије, односно физичку удаљеност одређених радних станица;

36. Да ли се и који део посла са ИТ системима *outsource*-ује (које су то компаније и који је опис посла који обављају код вас)?

2018. године 46% испитаних локалних самоуправа је пријавило да за одржавање апликација и мрежа које нису под директном контролом локалних самоуправа (као што су систем ЛПА, ЦЕОП и сл.) ангажује екстерне компаније, док је друга половина навела да не користи *outsourcing* услуге. Ове године 54% испитаних

локалних самоуправа наводи да *outsource*-ује део посла из надлежности ИТ сектора, док остатак то не чини. *Outsource*-ује се одржавање система, сервисирање опреме, одржавање веб презентације, мрежне инфраструктуре итд. И ово питање показује тенденцију ЛС да ангажују екстерна лица за помоћ у одржавању ИТ система;

37. Да ли су базе података ЈЛС заштићене довољно јаким лозинкама?

У 2018-ој 45 од 63 локалне самоуправе (односно 71%) су пријавиле да имају добро заштићене базе података и да користе лозинке са 8 или више карактера (укључујући велика, мала слова, бројеве и специјалне знакове). 15 ЛС (односн 24%) је сматрало да им лозинке нису довољно јаке. У 2019. години 44 од 69 локалних самоуправа (односно 64%) наводи да су заштићени јаким лозинкама, док 23 (односно 33%) сматра да им лозинке нису довољно јаке;

38. Да ли је у последњих годину дана било околности које су захтевале активацију *BCP* и *DRP*?

2018-е године 32 од 63 локалне самоуправе (односно 64%) су навеле да нису забележиле оклоности које су захтевале активацију *BCP* и *DRP*, док 3 (6%) јесу. Ове године је већина прескочила ово питање, док је неколико њих нагласило да није упознато са овим скраћеницама. Неки су навели да нису имали озбиљнијих прекида у раду, те да за активацијом *Business Continuity* и *Disaster Recovery* плана није било потребе. Само две локалне самоуправе (3%) су на ово питање дале потврдан одговор;

39. На којој локацији се налази примарни рачунарски центар на коме се налазе главне пословне апликације? На којој локацији се налази резервног рачунарског центра на којој се налазе главне пословне апликације? На којој локацији се налазе остали рачунарски центари које локална самоуправа користи?

У обе анализе готово већина локалних самоуправа је навела да се примарни рачунарски центар налази у згради локалне самоуправе, односно у сервер сали; Обе анализе су показале да већина локалних самоуправа нема резервни рачунарски центар, док оне које имају га махом смештају на истој локацији где се налази и примарни;

2018. године је 75% локалних самоуправа навело да нема резервни рачунарски центар, а ове године 76% и више (сви који су одговорили „ниједан од понуђених одговора“ у објашњењу су нагласили да немају резервни рачунарски центар). Од оних које су навеле да имају, 2018. године 2 (3%) пријавиле су да је у питању пресликани рачунарски центар, док је 1 (2%) навела да има *warm site*. Нешто више ЛС ове године наводи да има или пресликани резервни рачунарски центар, или да имају *hot site* или *warm site* (укупно 11%).

40. Којим збиркама података о личности располаже Ваша ЈЛС и по ком правном основу? Ко су корисници ваших збирки података о личности и по ком основу?

2018. године већина ЈЛС је наводила да располаже матичним књигама, бирачким списковима и кадровским евиденцијама као збиркама података о личности којима

располажу. Наводиле су и евиденције о пореским обвезницима локалних јавних прихода, евиденције о држављанима, расељеним и избеглим лицима, корисницима стипендија и дечијих додатака, евиденцијама о предузетницима итд. Ове године је већина избегла одговор на ово питање, док су оне које су одговориле навеле да располажу различитим интерним евиденцијама запослених, као и евиденцијама које се воде на основу закона;

У 2018. години су ЈЛС наводиле следеће кориснике збирки података о личности: интерно – овлашћена лица за вођење евиденција, руководиоце одељења у локалним самоуправама, матичаре и сл, а екстерно грађане и правна лица по захтеву, као и полицију и стручне службе по захтеву. Ове године су одговори углавном неодређени попут „подаци су доступни за јавност“, „подаци садрже прописани степен тајности и нису доступни другима“, „подаци су јавни осим у случајевима прописаним законом“... Као корисници навођена су министарства и други државни органи, лица на која се подаци односе и овлашћени службеници.

41. Које су мере заштите података о личности предузете у оквиру Ваше ЈЛС?

2018. ЈЛС су наводиле да приступ подацима о личности имају само службеници који су задужени за одржавање базе или евиденције уз лозинку, да се сервери налазе у посебним просторијама и да, уколико су подаци у папирном облику да се налазе у закључаним просторијама. 4 су навеле да немају посебне мере заштите. Ове године су сем побројаних навођене и следеће мере: чување података на посебним рачунарима, дежурно лице које чува збирке података и видео надзор. Неколико локалних самоуправа је навело да њихови акти не садрже такве податке који би изискивали посебну заштиту или да нема посебних мера заштите;

ПРЕПОРУКЕ

На основу анализе резултата истраживања издвојено је неколико препорука за унапређење превенције у области информационе безбедности локалних самоуправа и координације извештавања и одговарања на инциденте.

1. **Потребно је да се што раније све јединице локалне самоуправе повежу на јединствену информационо-комуникациону мрежу електронске управе (ЈИК мрежу)** у складу са чланом 8. Закона о електронској управи, како би били обухваћени заштитом коју пружа Канцеларија за ИТ и еУправу, као ЦЕРТ републичких органа задужен за заштиту од инцидената у оквиру ЈИК мреже. До краја 2019. на ЈИК мрежу било је повезано само 20% локалних самоуправа. Предлогом програма развоја електронске управе за период 2020-2022. предвиђено је да 40% њих буде на ЈИК мрежи до краја 2020.
2. Будући да велики број локалних самоуправа користи застареле софтвере, системе и апликације, као и бесплатне верзије антивирус програма, неопходно је донети **смернице Канцеларије за ИТ и еУправу о препорученим софтверима**. Неопходно је планирати додатна улагања и определити средства како би све локалне самоуправе имале обезбеђена средства за рад у савременим и безбедним условима – минимум у виду лиценцираних програма који се користе у

свакодневном раду, као и новије верзије оперативних система са подршком. Ово је посебно важно будући да локалне самоуправе у великој мери користе Windows 7 (97%) као и Windows XP (62%) за које је престала подршка, и да многе локалне самоуправе користе нелиценциране софтвере.

3. Неопходно је систематизацијом радних места предвидети да **најмање један запослени обавља послове администратора система и администратора мреже**, како би се могле адекватно спроводити мере заштите и координирати све активности и одговорности локалне самоуправе према Закону о информационој безбедности и Закону о електронској управи. Истраживање показује да четвртина локалних самоуправа нема организациону јединицу задужену за ИТ послове у локалној самоуправи, а 20% локалних самоуправа нема запослено ИТ лице.
4. Резултати анкете показују да већина локалних самоуправа никад није проверавала информациону безбедност својих система. У недостатку интерних капацитета и средстава за ангажовање комерцијалних услуга провере информационих система, **предлажемо успостављање мреже запослених/ задужених за ИТ у локалним самоуправама (уз подршку ЦЕРТ-а републичких органа), који би били у прилици да на заједничкој платформи[1] размењују информације, знања и искуства и једни другима обављају редовну екстерну проверу информационих система.** Успостављање овакве платформе би допринело уједначавању уређивања и примене процедура за мере из акта о информационој безбедности у различитим локалним самоуправама, унапређењу размене информација и сарадње појединачних локалних самоуправа са надлежним ЦЕРТ-ом и успешније заговарање подизања капацитета за успостављање безбедне и ефикасне електронске управе на локалу. Ово је посебно важно и због чињенице да је неопходно унапредити и доследно спроводити политику логовања на систем, односно користити двофакторску аутентикацију, користити јаче лозинке (8 или више алфанумеричких карактера, коришћење великог слова, специјалних карактера), као и мењати лозинке на минимум 45 дана, што се у пракси недовољно спроводи.
5. Како би Канцеларија за ИТ и еУправу била у могућности да адекватно штити мрежу органа јавне управе, потребно је општим актима **успоставити јасне процедуре за управљање, коришћење и заштиту ЈИК мреже, мрежни оперативни центар (енг. *Network Operation Center - NOC*), оперативан ЦЕРТ републичких органа и тим за одговор на инциденте (енг. *Incident Response Team*) и аналитику за учење на грешкама** у складу са извештајима ИКТ система од посебног значаја. Услов за наведено је да Канцеларија за ИТ и еУправу подигне стручне капацитете и успостави организационе јединице које ће обављати претходно наведене послове или управљати овим пословима у случају да се определи за екстерне стручњаке.
6. Канцеларија за ИТ и еУправу у сарадњи са инспекцијом за информациону безбедност би требало да прати спровођење обавеза из Закона о информационој безбедности од стране органа јавне управе и издаје **смернице за интерне**

[1] Платформа би требало да буде заштићена применом *SSL/TLS* технологије веб страница и комуникација би требало да буде енкриптована.

процедуре и стандарде како за превенцију, тако и за поступање по претњама и инцидентима којима буду изложени. Посебно бисмо нагласили потребу за дефинисањем јасних и уједначених процедура за опоравак у случају катастрофа и обезбеђивање континуитета пословања, с обзиром да их скоро ниједна локална самоуправа није донела, а ниједна их није тестирала у претходних годину дана. Наиме, Закон о информационој безбедности прописује обавезу свих ИКТ система од посебног значаја, па и јединица локалне самоуправе, да донесу Акт о информационој безбедности и пратеће процедуре за свих 28 мера безбедности. Како би се избегла неуједначеност у примени, пожељно је да се процеси који су релативно слични у свим локалним самоуправама уреде на уједначен начин, што ће омогућити примену најбоље праксе и олакшати управљање системима и одговор на инциденте. Будући да Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја уопштено прописује мере заштите, неопходно је да Канцеларија за ИТ и еУправу донесе смернице по којима би локалне самоуправе поступале, нарочито за израду Плана за обезбеђење континуитета пословања и Плана опоравка од катастрофа, чију израду сугерише Национални ЦЕРТ у свом Моделу акта о информационој безбедности. На основу утврђеног стања и праћења примене ових смерница **потребно је да се обавезне процедуре за органе јавне управе стриктније пропишу допуном Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја**.

7. Иако је Канцеларија за ИТ и еУправу ЦЕРТ републичких органа задужена за заштиту ЈИК мреже, Закон о информационој безбедности прописује да оператори ИКТ система од посебног значаја обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности врше преко веб странице Министарства трговине, туризма и телекомуникација (МТТТ) или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима. Поред тога, према Закону о заштити података о личности неопходно је у року од 72 сата од инцидента којим су угрожени подаци о личности обавестити Повереника за информације од јавног значаја и заштиту података о личности, а уколико постоје основи сумње да је учињено кривично дело, неопходно је обавестити и полицију, односно поднети и кривичну пријаву Тужилаштву за високотехнолошки криминал. Посебно бисмо нагласили да је за разлику од Националног ЦЕРТ-а, обавеза ЦЕРТ-а републичких органа и реаговање на сваки напад у оквиру ЈИК мреже, а не само његово евидентирање. Како је код инцидената и успешног реаговања најважније време, **потребно је успоставити механизам за једноставно обавештавање и координацију Националног ЦЕРТ-а, ЦЕРТ-а републичких органа, МУП-а, других ЦЕРТ-ова и Повереника за информације од јавног значаја и заштиту података о личности**. Потребно је додатно прецизирати Закон о информационој безбедности[2] на начин да сви (па и локалне

[2] Члан 18. став 2 Закона о информационој безбедности прописује координацију и сарадњу са операторима ИКТ система које повезује јединствена мрежа у превенцији инцидената, откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената, што и даље не подразумева пријаву инцидената локалних самоуправа као оператора ИКТ система повезаних на ЈИК

самоуправе) инциденте пријављују преко јединствене платформе, на коју су повезани сви претходно наведени органи, а како би у најкраћем року била обезбеђена адекватна подршка и како би се спречила штета већих размера. На овај начин би локалне самоуправе једном радњом испуниле своје законске обавезе пријављивања инцидента и Националном ЦЕРТ-у и Поверенику и Тужилаштву за ВТК, укључујући и пријаву свом ЦЕРТ-у, који треба да обезбеди заштиту ЈИК мреже, а којем по садашњем законском решењу нису обавезни да пријаве инцидент. С друге стране, успостављањем јединствене приступне тачке за пријаву свих врста инцидената Национални ЦЕРТ може имати много бољи преглед свих инцидената који се сада пријављују различитим ЦЕРТ-овима и на основу њих дефинисати ажурне периодичне извештаје о стању информационе безбедности са препорукама за даље унапређење и превентивно деловање ИКТ система од посебног значаја. Исто тако, Повереник за информације од јавног значаја и заштиту података о личности на овај начин може имати ажурнији и правовремен преглед стања и ризика кад је реч о заштити података о личности и тако бити ефикаснији и у надзору и у дефинисању превентивних мера.

мрежу Канцеларији за ИТ и еУправу. Члан 11, који дефинише обавезу пријаве инцидената, не прописује пријаву ЦЕРТ-у републичких органа и зато је неопходно прецизирати ЗИБ.

ЗАКЉУЧАК

Из приложених резултата истраживања приметно је да је мало тога унапређено у односу на 2018. годину када је реч о информационој бебедности. Будући да се 49% узорка поклапа са претходним истраживањем, у прилици смо да пратимо развој тих локалних самоуправа, али и да податке освежимо са већином нових (51% узорка је различито у односу на претходну годину).

Позитиван помак је изражен у односу ИТ лица наспрам укупног броја запослених који је у 2018. години износио 1/65, а сада износи 1/62. Резултати одговора на остала питања су у великој мери слични одговорима из истраживања спроведеног 2018. године. Разлике су мање или без већег значаја за укупан резултат.

Скрећемо пажњу на неколико напомена у вези са резултатима истраживања. Наиме, поред потребе усвајања Акта о информационој безбедности, важно је нагласити да Акт садржи 28 мера заштите које би требало да служе као основ за дефинисање и примену процедура за поступање у складу са сваком мером појединачно. Дакле, када се говори о доследној примени Акта, потребно је имати у виду све мере и процедуре које из Акта произлазе.

Када је реч о ангажовању екстерних компанија за одржавање мрежа и/или система, неопходно је применити све могуће мере ради заштите података у личности у складу са важећим Законом о заштити података о личности („Сл. гласник РС“, бр. 87/2018), а поготову оне које се односе на израду процене утицаја предвиђених радњи обраде на заштиту података о личности у складу са чланом 54. овог закона.

Општи закључак је да се мало пажње посвећује проблему информационе безбедности и да би требало радити на његовом унапређењу. Из резултата истраживања произлази да су главни проблеми са којима се суочавају локалне самоуправе када је реч о информационој безбедности следећи:

- недостатак ИТ кадра;
- недостатак техничких и финансијских ресурса;
- застарела опрема;
- крхки системи и мреже.

Приметна је и слаба координација у одговарању на инциденте. Из тог разлога су дате и препоруке за унапређење превенције у области информационе безбедности локалних самоуправа, као и побољшање ефикасности у извештавању о инцидентима и реаговању на инциденте, међу којима су: повезивање на јединствену информационо-комуникациону мрежу (ЈИК мрежа), успостављање јасне процедуре за управљање, коришћење и заштиту ЈИК мреже, успостављање мрежног оперативног центра (енг. *Network Operation Center - NOC*), оперативног ЦЕРТ-а републичких органа и тима за одговор на инциденте (енг. *Incident Response Team*) и за аналитику за учење на грешкама у складу са извештајима ИКТ система од посебног значаја. Ово такође подразумева и израду смерница за интерне процедуре и стандарде у превенцији и у поступању по претњама и инцидентима од стране Канцеларије за ИТ и еУправу. Смернице је неопходно донети и у погледу препоручених софтвера као и планирати додатна средстава и улагања, будући да су налази истраживања показали да већина локалних самоуправа користи и оперативне системе без подршке и нелиценциране

верзије софтвера. Неопходно је систематизацијом радних места предвидети да најмање један запослени обавља послове администратора система и администратора мреже. Такође је важна и размена искустава ради обављања екстерне ревизије система, те се предлаже успостављање заједничке платформе, односно мреже ИТ лица локалних самоуправа. Најзад, како је код инцидената и успешног реаговања најважније време потребно је успоставити механизам за једноставно обавештавање Канцеларије за ИТ и еУправу и координацију овог ЦЕРТ-а Националним ЦЕРТ-ом, МУП-ом, другим ЦЕРТ-овима и Повереником за информације од јавног значаја и заштиту података о личности.

Имајући у виду да ове године истиче примена постојеће Стратегије развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године, надамо се да ће ова анализа и дефинисане препоруке користити у изради нове стратегије и разради мера и активности њеног акционог плана.