

АНАЛИЗ

на резултатите от Изследване и мониторинг на ефективното прилагане на Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС) от 16 общини първа, втора и трета категория

1. УВОД

Настоящия анализ е разработен в съответствие с дейностите планирани за извършване в рамките на дейност 1, „Изследване и мониторинг на ефективното прилагане на НМИМИС от общини първа, втора и трета категория“, по проект BG05SFOP001-2.025, с наименование „Повишаване на общото ниво на мрежова и информационна сигурност в общински администрации“, Дейността обхваща 5 общини първа категория, 5 общини втора категория и 6 общини трета категория.

Основните цели на този анализ са:

а) да се идентифицират и анализират общите предизвикателства и рискове за мрежовата и информационната сигурност (МИС), пред които е изправена всяка една категория общини, като се вземат предвид и евентуални специфичности в тяхната дейност.

б) Въз основа на самооценката, предоставена от участващите общини, екипа за изпълнение на проекта да представя моментна снимка на имплементацията на НМИМИС в трите категории общини, като се обърне внимание на ключови елементи, които допринасят за киберустойчивостта на общините. Посочване на добри практики, изведени като отправени препоръки с което ще се подпомогне процеса за преодоляване на „препятствията“ и бариерите пред български общини. Така същите ще бъдат подпомогнати в усилията им за привеждане на техническите им, общински и процесни ресурси в областта на мрежовата и информационна сигурност, в съответствие с изискванията.

в) Да се засили връзката между НПО сектора, в лицето на Българска асоциация по киберсигурност и представителите на общинската власт.

Този анализ се фокусира върху вътрешните механизми създадени за управление на системи за МИС в общините, които са предназначени да защитават техните ресурси в киберпространството и да гарантират изпълнение на възложените им функции.

Анализа не претендира, че дава пълна оценка на състоянието на МИС, на надеждността на работа механизмите и/или техническа инфраструктура на всяка община, и по-скоро има за цел да даде представа за общите налични възможности и да подчертае някои общи въпроси, които може да заслужават специално внимание.

Анализа не се опитва да даде и окончателна оценка на цялостната степен на развитие на МИС в общините. Освен това екипът счита, че оценката би имала ограничена практическа стойност, тъй като сравнението с други общини или „усреднена“ оценка за нивото на МИС няма да даде необходимата пълнота от информация.

За по-голяма прецизност при използването на понятията за различните видове общини, в съответствие с използваната от Министерство на регионалното развитие и благоустройството и за целите на проекта, екипът използва терминология „общини първа категория“, вместо „голям тип община“. Аналогичен е подхода и за другите две категории общини.

Стремежа на екипа по време на изготвяне на анализа беше, да се използва специализирана терминология в съответствие със Закона за киберсигурност (ЗКС).

Съществуват и свързани области на обработка на данни, които са от значение за МИС, но те са извън обхвата на анализа.

Екипът в своята дейност се съобрази с ограничения, свързани с поверителност на данните за заплахите, инциденти и по-специално мерките за реагиране, тъй като обменът на

такава информация създава ненужен риск, свързан с идентифицирането и излагане на уязвимости на общинската инфраструктура за сигурност, така че информацията е представена предимно в обобщена форма, без посочване на конкретни данни и информация.

По очевидни причини, свързани с предмета на този анализ, в съответствие с предварително декларирания ангажимент, екипът на нито един етап от своята дейност не разкрива данни за състоянието на МИС в конкретна община, тъй като това може да застраши безопасността им.

Посочените оценки в настоящия анализ, отнасящи се до Вашата община се съдържат само в екземпляра изпратен до Вас и няма да бъдат предоставяни на други лица.

С оглед обхвата на изследването и целевата група към която е насочено същото в анализа, екипът по дълбоко свое вътрешно убеждение обърна по-голямо внимание на изискванията за всеобхватни и адекватни, пропорционални и подходящи организационни мерки, като в приоритетните изисквания са цитирани и някои добри практики по повишаване нивото на МИС.

Техническите аспекти не са анализирани в детайли. Въпреки че МИС не е чисто технически проблем, той не може да бъде решен без да се вземе предвид неговият ИКТ аспект. Пред екипа обаче не е стояла такава задача. Поради това не са анализирани задълбочено предприетите мерки от обините, по отношение на тяхната техническа и технологична адекватност или надеждност.

По отношение на технологичния и експлоатационен капацитет на общините в сферата на ИКТ, екипът се ограничи до подчертаване на някои проблеми, свързани с остатъци от наследени системи, придобити в миналото или създадени вътрешно във времето, които може вече да не се поддържат от съвременни инструменти за проверка на сигурност и решения; продължаващото разширяване на използването на облачна среда; организационни механизми за анализиране и преодоляване на уязвимостите; както и използването на сенчести информационни технологии (shadow IT), в т.ч използване и внедряване на технологични средства извън информаионни и комуникационни системи (ИКС).

За постигане на поставените цели, екипът за изпълнение на Проекта използва набор от следните качествени и количествени методи за събиране на данни от различни източници:

- 1) Кабинетно проучване на относимата за проекта, стратегическа и нормативна уредба;
- 2) Създаването на въпросник, отговорите, по които да създадат условия за оценка нивото на интеграция на НМИМИС от трите категории общини;
- 3) Провеждане на 3 фокус групи с представители на трите категории общини натоварени с техническото имплементиране на НМИМИС;
- 4) Провеждане на 6 интервюта с ръководители на общински администрации (или определени от тях лица) – по двама представители от всяки тип община.

Екипът провери приложимата правна и регулаторна рамка след което беше създаден въпросник, който обхваща всички изисквания на НМИМИС, включително и приложенията към нея, релевантни на спецификите в общини.

Подготвените въпроси предполагаша конкретни и ясни еднозначни отговори в съответствие със спецификата на местната администрация (въз основа на нейния статус, информацията, която тя притежава или контролира, потенциални рискове, ресурси и т.н.). В същото време беше взето предвид, че общините не са изолирани и в много отношения са взаимосвързани, както с други общини така и с други публични органи. Включително и в резултат на съвместно разработване и изпълнение на програми от тях. Ето защо беше изключително важно да се определят евентуални зони на общи слабости.

Въз основа на попълнени Въпросници, екипът организира провеждането на 3 фокус групи със служители отговарящи за МИС От общините където няма определен такъв служител, участва определен от ръководството ИТ персонал. Проведени са последващи интервюта с 6

ръководители на общински администрации (или определени от тях лица) – по двама представители от всяка категория общини.

За извършване на оценка и анализиране степента на имплементиране по отговорите предоставени от изследваните общини в съответствие с изпратения им въпросник беше разработена Методология за изследване и мониторинг на ефективното прилагане на НМИМС от общините 1, 2 и 3 категории, участващи в Проект - BG05SFOP001-2.025 „Повишаване на общото ниво на мрежова и информационна сигурност в общински администрации“.

С цел улесняване последващите дейности на общините за персонализиране на направените констатации, изводи и препоръки в анализа, същия е разработен със структура в основната си част, идентична на тази на въпросника. Т.е. точките от 1 до 33 в двата документа са еднакви.

Предвид огромния разнороден масив от информация (над 3000 записа, които са интегрирани в три общи таблици, по тях са направени графики, констатации, изводи и препоръки) и въпреки положените усилия от екипа е възможно да има допуснати някъде несъществени грешки.

В анализа при посочването на определен брой общини –изпълнили съответните изисквания на НМИМС (или неизпълнили), следва да се има предвид, че в повечето случаи става дума за различни комбинации от по 5 (6) общини.

2. ОСНОВНА ЧАСТ

В основната част са показани общите резултати самостоятелно за всяка една от трите категории общини в оценка по шестобалната система. Оценка се отнася за степента на изпълнение на НМИМС и са интегриран резултат от оценките по отделните изисквания. по съответните раздели, глави и части.

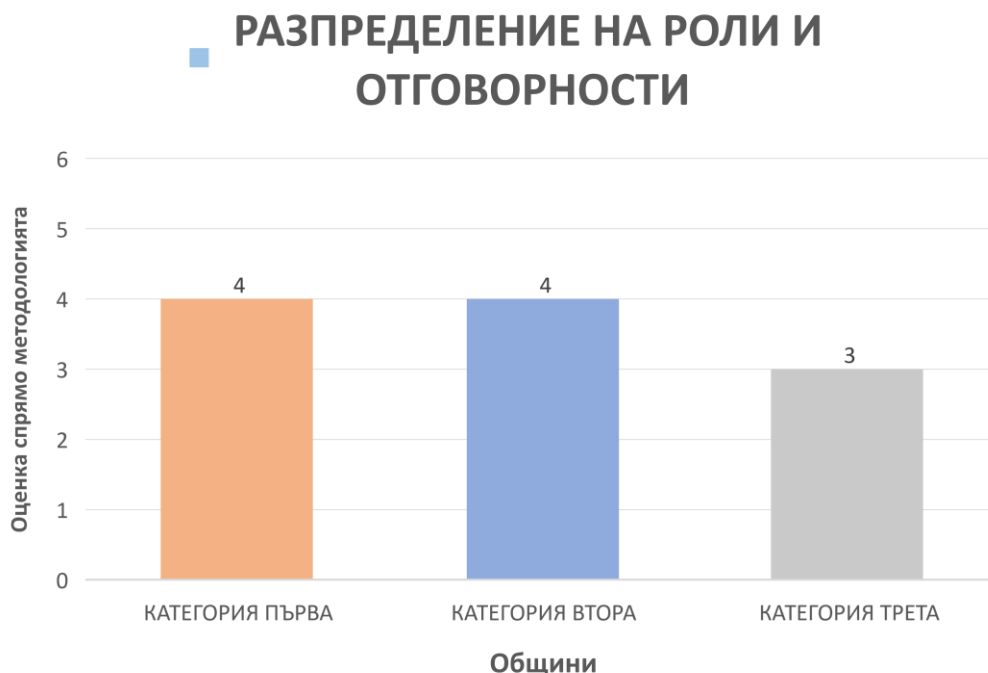
Глава първа – Общи положения (по нея няма въпроси и съответно резултати)

Глава втора – Минимални мерки за мрежова и информационна сигурност

Раздел I – Управление на мрежовата и информационната сигурност

1. Разпределение на роли и отговорности

Резултати:



Фигура 1 Резултати от проведено проучване по т. Разпределение на роли и отговорности.

КОНСТАТАЦИИ:

- От така получените резултати е видно, че 2 (от общо 5) от общините първа категория, оценяват важността на мерките по този въпрос. В тези общини са определени във връзка с чл.3, ал.2 от НМИМИС служители отговарящ за МИС и е извършен годишен преглед на МИС и адекватността на приложените мерки, за 2022г.

- Половината от общините втора категория са изпълнили изискване, като 4 (от общо 5) са определили служители отговарящ за МИС, а само една е извършила годишен преглед на МИС за 2022 г.

- По-малко от половината общини трета категория изпълняват това изискване. Там едва 2 (от общо 6) са определили служители отговарящ за МИС и 2 са звършили – ежегоден преглед на МИС за 2022 г.

ИЗВОДИ:

- В част от общините, МИС се възприема като предимно технически проблем. Поради това целенасочено в изследването се взема предвид и степента на участие на ръководствата на общини (имат се предвид кметове, зам.кметове, секретари) по тази тема или участието им в разглеждането ѝ.

- Половината 8 (от общо 16) от участващите общини са определили с нарочна заповед служител отговарящ за МИС, т.е. налице са човешки ресурси за тази цел, като с изключение на една община, тези отговорности се възлагат на служител от ИТ персонала към основните функционални задължения по съвместителство. Т.е. в тези общини отговорността по МИС лежи на плещите на ИКТ специалистите заедно с другите им задължения. В областта на МИС често се налага да участват и експерти от трети страни поради техническата и сложност и непрекъснато развитие, което изисква много специализирани знания. Придобиването, поддържането и усъвършенстването на тези знания е трудно, но невъзможно за осигуряване. Използването на ресурси от външни доставчици на услуги в областта на МИС понякога е неизбежно, а в отделни случаи и дори желателно за да бъдат общините в крак с бързо променящите се реалности в киберпространството. Степента в която това се прави, следва да зависи от внимателната преценка на всеки кмет в светлината на неговите задачи и условия. Според екипа обаче е важно общините да поддържат подходяща степен на контрол, надзор и технически капацитет в тях, за ефективно използване на потенциала, предоставен от руктури на трети страни, и взаимодействие с тях. В тази връзка, възможността за възлагане на тези задачи на служител по мрежова и информационна сигурност гарантира, че тази цел е може да бъде надеждно постигната. Основните функции имащи отношение към МИС и които са отговорност на старшия служител (например началника на отдел) отговарящ за ИКТ надхвърлят разработването на оперативни контроли и по подразбиране включва управленски аспект, за да се гарантира, че отразяват възможно най-пълно съображенията за МИС като проблем на управление на риска и устойчивост на общината.

ПРЕПОРЪКИ:

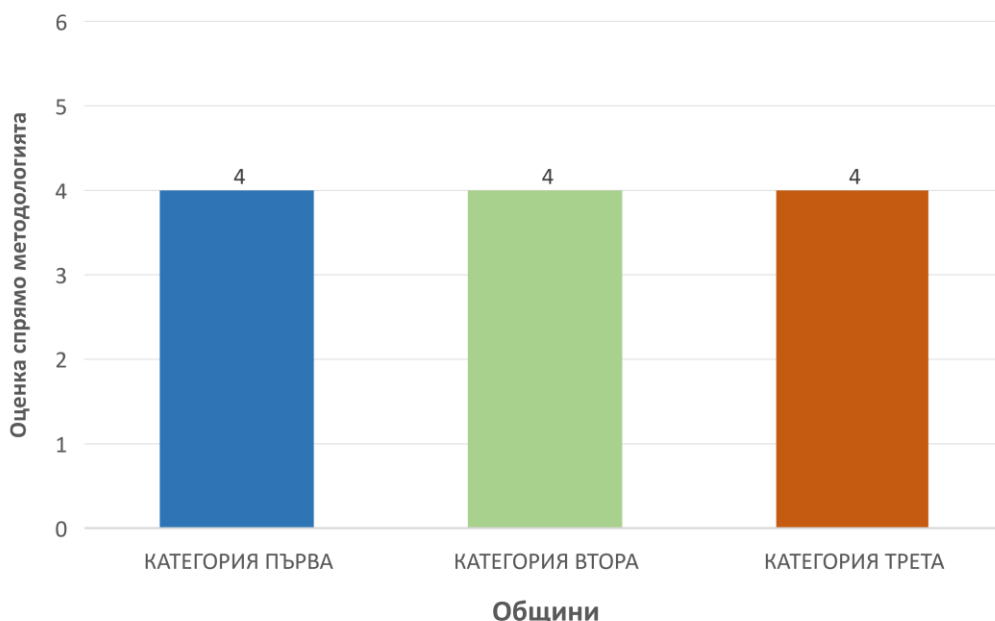
- В общините където няма определен служител отговарящ за МИС, ръководителите да предприемат мерки за определянето на такъв с нарочна заповед.

- Определянето на такъв служител от ИТ персонала който да изпълнява тези функции по съвместителство е НЕпрепоръчително.

3. Политики за сигурност

Резултати:

■ ПОЛИТИКИ ЗА СИГУРНОСТ



Фигура 2 Резултати от проведено проучване по т. Политики за сигурност.

КОНСТАТАЦИИ:

- В четири от общините първа категория са разработени Политиия за сигурност, а в една от тях не е разработена и приета такава.
- Броя на общините втора категория разработили приели, и съответно не разработили Политика за сигурност е идентичен с броя общини първа категория, т.е. 4 и 1.
- При общините трета категория броя на тези които са разработили Политика е 3 бр., а неразработилите политика е също 3бр.

ИЗВОДИ:

- Наличието на разработена и приета в съответствие с изискванията на чл.4 от НМИМС, Политика за сигурност е ключово и от първостепенно значение за състоянието на МИС във всички субекти на ЗКС, включително и за общините.
- В тази връзка екипът счита, че в общините където няма Политика за сигурност, са налице предпоставки за сериозни пропуски и за мащабни киберинциденти, като някои от тях може да доведат до загуба на различна по тип информация. Дори да се предприемат някакви други мерки освен тези които следва да бъдат предвидени в Политиката, то те биха имали частичен, палиативен и заблуждаващ характер, че е постигнато добро ниво на МИС.
- Липсата на такава Политика предполага и липса на съответни мерки за осигуряване на МИС на ИКС, при обмен на информация; при работа с мобилни устройства, при работа от разстояние, при използване на криптографски механизми; при управление на достъпите и автентификацията, при разработване на нови ИКС, при взаимоотношенията с трети страни, за повишаване квалификацията на служителите и на осведомеността им по въпросите на МИС и др.
- При разработване регулаторната рамка, необходима за подобряване на киберустойчивостта на общините би било нежелателно да се разглеждат само правилата, специално посветени на ИКТ и МИС. Поддържането на високо ниво на МИС на общината е обичайно отговорност на много структурни звена и отношението към нея като към корпоративна задача, може да бъде от голямо значение за постигане на вътрешно зрял, а не наложен подход за цялата община.

- Обхватът на изследването не обхваща въпроси дали в някои общини вече са започнали да включват съображения за МИС в своите различни (административни) политически документи.

ПРЕПОРЪКИ:

- Екипът най-настойтелно препоръчва на ръководството на общините в които не е разработена и приета Политика за сигурност, да предприемат адекватни и своевременни мреки за изготвянето на такава. Още повече, че тук става дума за организационни мерки, която не изисква финансови разходи (или ако изисква такива при липса на собствен ресурс, то те биха били пренебрежително малки).

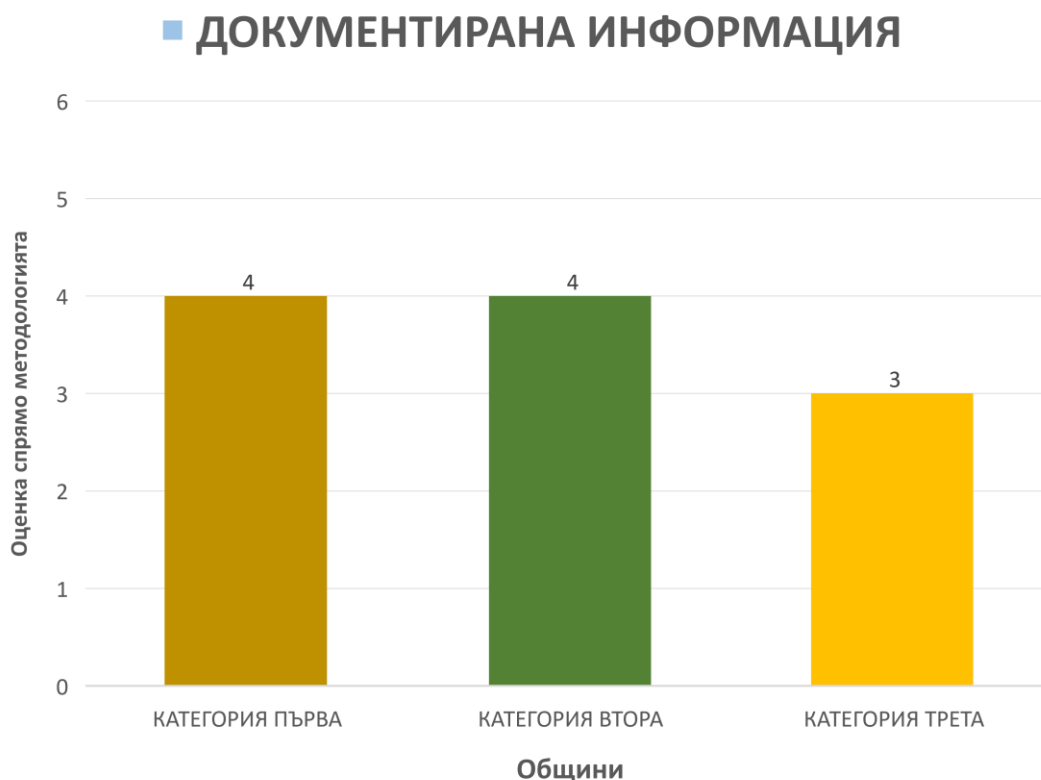
- В правилата, практиките и процесите, от които се ръководят в дейността си структурни звена като човешки ресурси, обществени поръчки, ПР, правен, да бъдат включени (когато е приложима) елементи, свързани с МИС.

- Включването в инструкции (вътрешни правила) за доставки, на специфични изисквания относно МИС. Специфични правила при ангажиране на външни доставчици на услуги, също следва да намерят място.

- Включване на стъпки, в проектни документи отнасящи се до ИКС или в документи за ръководство, използвани от структурните звена в тяхната ежедневна дейност които да се следват при управлението на рискове по МИС през целия жизнен цикъл на проекта.

4. Документирана информация

Резултати:



Фигура 3 Резултати от проведено проучване по т. Документирана информация.

КОНСТАТАЦИИ:

-По три общини от първа и втора категория са декларирали, че спазват изискванията относно документирането на информация съгласно изискванията на чл.5 от НМИМИС.

- Половината от общините трета категория са отговорили, че спазват като цяло изискванията за документиране на информацията. Изключение правят изискванията за наличие за схема на информационните потоци, за актуална документация на структурна кабелна ситема, на необходимата техническа, експлоатационна и потребителска документация на ИКС и компонентите им, изисквания за класифициране на информацията по чл.6 от НМИМС, по отношение регламентирането на достъпа до

- Документацията само на лицата чиито задължения налагат това. За тези изключения една единствена община е посочила, че отговаря на тях.

ИЗВОДИ:

- Разработването на изискуемата документация по чл. 5 от НМИМС в част от общините не стои на дневен ред.

- Подценени са ролята, значението и необходимостта от наличието на пълноценна документация, която да е основа за предприемане на своевременни, адекватни и пропорционални мерки за обезпечаване на МИС в общините.

- Достъпността до ясно формулирана документация за общините където тя е разработена и е налична е важно условие за спазване на НМИМС. За спазване на такива правила влияят няколко фактора, включително наличието на материали, в които ясно очертават какво се изисква от всяка заинтересована страна и всеки служител и защо. Проблемът не е толкова липсата на писмени инструкции, а лошото разбиране от страна на служителите, защото част от тези инструкции не показват, какво от МИС се защитава и как може да повлияе тяхното (на служителите) невежество и неспазването от тях в качеството им на потребители на установените правила. Важността на това осъзнаване включва необходимостта от просто, нетехническо и достъпно представяне на проблемите и мерките за разрешаването им и чиято основна задача е ясно да се очертаят последствията от рисковано кибер поведение за потребителя.

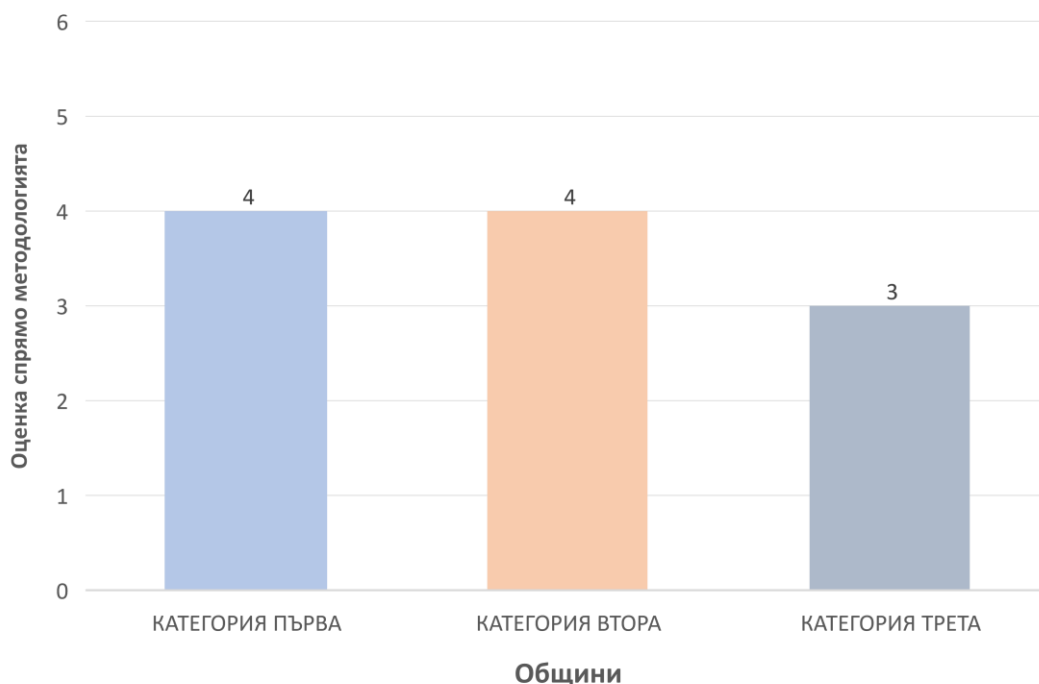
ПРЕПОРЪКИ:

- Екипът най-настоятелно препоръчва на ръководството на общините, в които не е разработена изискуемата по чл.5 от НМИМС документацията за сигурност, да предприемат адекватни и своевременни мерки за изготвянето на такава. Предвид факта, че тази документация е свързана с регулярна и рутинна дейност на ИТ служителите и ежедневната дейност на потребителите т.е. това са организационни мярки, за тях не са необходими финансови средства.

5. Класификация на информацията

Резултат:

■ КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА



Фигура 4 Резултати от проведено проучване по т. Класификация на информацията.

КОНСТАТАЦИИ:

- Четири от общините първа категория са изпълнили изискванията на НМИМИС, по чл.6,, ал1, ал.2 (Имат разработени вътрешни правила за класификация на информацията и тази класификация се прилага върху всички активи които участват в създаването, обработването, съхранението, пренасянето и унищожаването на информацията).

- Само една от общините от тази категория прилага класификацията TLP(Traffic Light Protocol - Прил.2), по чл.6, ал.7 от НМИМИС която се изолзва при обмен на информация.

- При две от общините не съществува разлика между класификация на информацията по НМИМС и съгласно Закона за защита на класифицираната информация;

- Резултатите за общините втора категория показват, че 3 от тях спазват изискванията по чл.6, ал.1, ал.2. и ал.5, от НМИМИС, а 2 общини – прилагат класификацията TLP.

- Половината от общините трета категория са декларирали изпълнение на изискванията та чл.6, ал1 и ал.2 от НМИМС. Нито една община не е приложила мерки за недопускане използването на нива за класификация за сигурност на информацията от обхвата на Закона за защита на класифицираната информация. Само две общини прилагат класификацията при обмен на информация TLP.

ИЗВОДИ:

- Преобладаващата част от общините (11бр.), изпълняват изискванията за създаване на вътрешни правила за класифициране на информацията и я прилагат върху съответните активи.

- Не такива са резултати по отношение на изискванията за недопускане използването на нива за класификация за сигурност на информацията от обхвата на Закона за защита на класифицираната информация и по отношение прилагането на класификацията TLP при обмен на информация, където само 6 и съответно 5 общини са отговорили положително. Причината тук според екипа е по-скоро неразбиране на същността на класификацията на информацията,

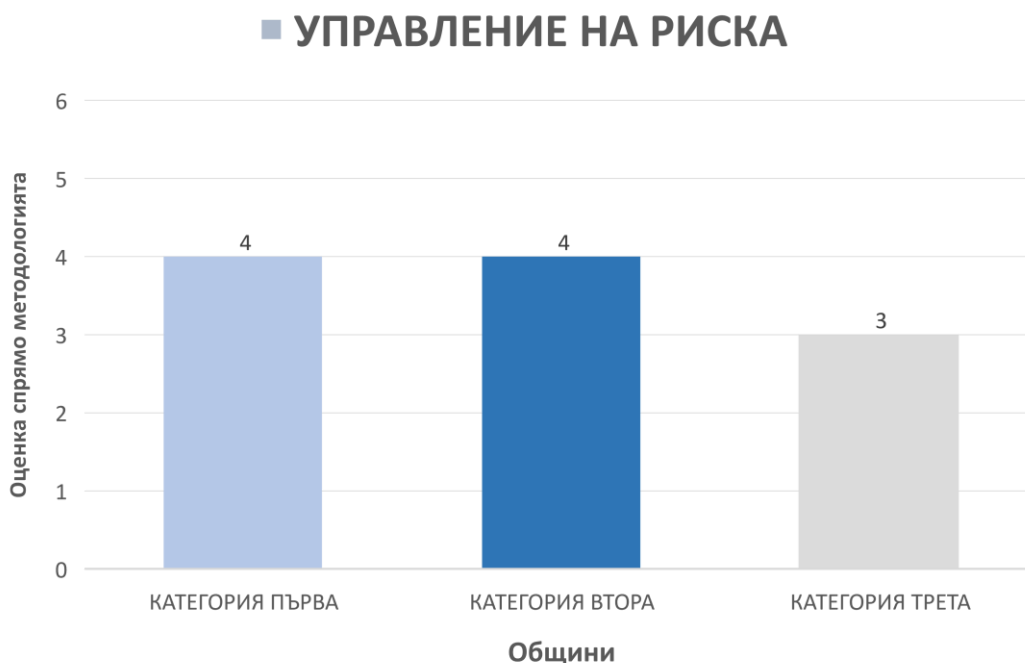
същността на класификация при обмен и релацията по този въпрос със Закона за защита на класифицираната информация.

ПРЕПОРЪКИ:

- Екипът смята, че не съществуват обективни обстоятелства които да възпрепятстват изпълнението на изискванията за класификация на информацията и по тази причина препоръчва да се предприемат организационни мерки за изпълнение на изискванията в общините където те не са изпълнение изцяло.

Резултати:

6. Управление на риска



Фигура 5 Резултати от проведено проучване по т. Управление на риска.

КОНСТАТАЦИИ:

- Една от общините първа категория е приложила мерки за изпълнение на всички изисквания за оценка на риска по чл.7 от НМИМИС, а останалите 4 общини са приложили мерки за по две от изискванията. Тези 4 общини не са приложили по едно от изискванията на чл.7.

- Повече от половината общини (3бр.) втора категория са отговорили, че са пизпълнили изискванията. Две общини не отговарят на тези изисквания.

- Три от общините са трета категория извършват оценка на риска по утвърдена на общинско ниво Методика и са извършили анализ и оценка на риска през 2022 г. План за подходящи и пропорционални мерки за смекчаване на риска има разработна само в една община.

- Управлението на риска в една община се характеризира като: структуриран процес в цялата община; цялостна и систематична идентификация на информационните активи; анализ, оценка, обработка и мониторинг на рисковете за МИС. Основни функции, свързани с МИС (обикновено опции за откриване, оценяване, предотвратяване, реакция и възстановяване на кибератаки и инциденти с МИС) отразяват ключовите етапи и цели на управление на риска. Третиране на МИС като проблем на управление рисковете на общинско ниво има от своя страна и специфични практически ползи. Първо, за да бъде признат за стратегическа цел на цялата община, следва: МИС да се превърне в приоритет, засягащ всички структурни звена и всички служители. Освен това екипът счита, че официалното включване на МИС в концепцията за

управление на риска в общината ще допринесе за оценяване важността на тази тема сред различните и приоритети и ще я превърне в официална начална точка, от която Ръководството на общината ще може да организира разработването на план за оптимално управление на основните рискове.

- Не на последно място сред констатциите екипът смята за необходимо да подчертае специално, че управлението на риска за МИС е залегнало в основата от дейности предвидени в Закона за киберсигурност. Във влязлата в сила Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза, на мерките за управление на риска също е отделено специално внимание.

ИЗВОДИ:

- Липсата на Методика за оценка на риска утвърдена от общината, неизвършена оценка на риска и липсата на План с мерки за смекчаване на риска предполагат и невъзможност за предприемане на проактивни мерки за постигане на по-високо ниво на МИС. Всички тези липси предполагат и неприемливо ниво на изпълнение на тези изисквания за МИС.

- Документите свързани с управлението на риска, трябва да позволяват систематичен и периодичен преглед, адаптиране и индивидуализиране на мерките за намаляване на рисковете в светлината на променящите се изисквания на общината. .

- Парадигмата за управление на риска в МИС е призната. полезност при разглеждане на МИС през призмата на цялостното управлението на риска.

- Следва изрично да се подчертае, че актуалните версии на стандарти за киберсигурност, включително ISO/IEC7001, и стандарти на Националния институт за стандарти и технологии на Съединените щати, вземат предвид рисковете за МИС преди всичко като организационни рискове, които отиват далеч отвъд критичните информационни инфраструктури и подчертават стратегическия аспект на подобряването състоянието на МИС в организациите (общините). Най-добрият начин за това е постигането на пълна корелация с управлението на другите видове риск на общинско ниво.

- Ръководството на общините трябва да се интересува и да е наясно като минимум с основните стратегически рискове, пред които е изправена общината, както и стратегии и механизми за тяхното управление. Според екипа, това трябва да включва ангажираност и лидерство в областта на МИС, предвид нейния критичен характер не само като проблем при управление на риска, но и като ключов фактор за изпълнение на функциите на общините..

- Установяване на ясни насоки относно приемливия риск за общината в проблеми с МИС, е свързано и с директно определяне на степента на риск, който се считат за приемливи в конкретния контекст.

ПРЕПОРЪКИ:

- Екипът смята, че изискването за прилагане на мерки свързани с управление на риска за МИС в общините е също особено важно поради което, препоръчва ръководствата на общини в които не са изпълнени едно или повече от изискванията по чл.7 от НМИМИС, „Управление на риска“, да предприемат подходящи и пропорционални мерки за изпълнението им. Мяроките са организационни и не предполагат необходимост от допълнителен финансов ресурс.

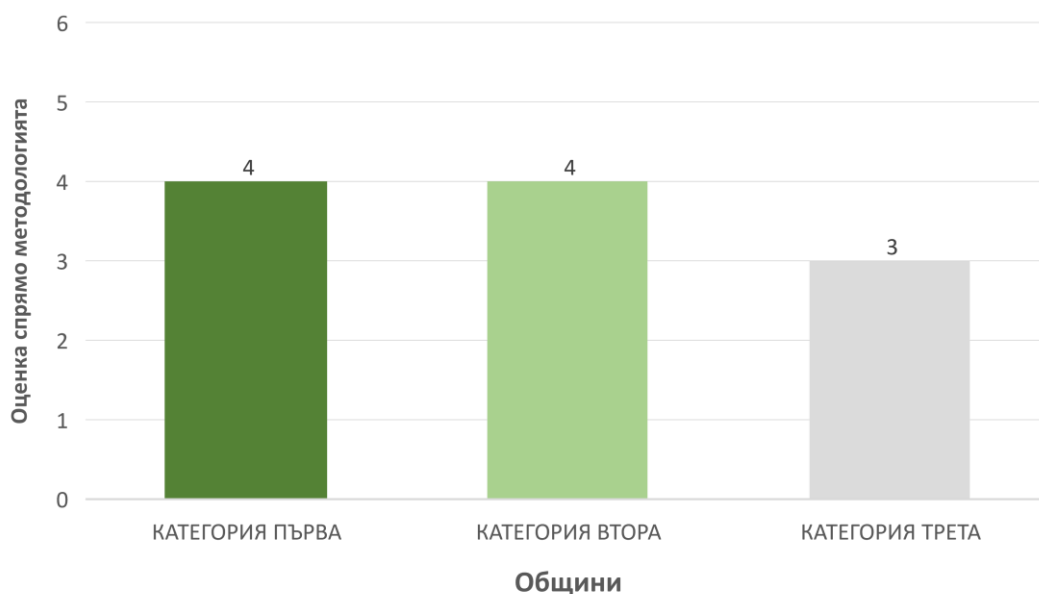
- Всички дейности свързани с анализ и оценка на риска за МИС следва да са релевантни и на цялостната дейност на общината по управление на риска за останалите сфери от нейната дейност.

- Общините които нямат приета Методика за оценка на риска, биха могли да използват примерната такава от НМИМИС, Прил.7

7. Управление на информационните активи

Резултати:

УПРАВЛЕНИЕ НА ИНФОРМАЦИОННИТЕ АКТИВИ



Фигура 6 Резултати от проведено проучване по т. Управление на информационните активи.

КОНСТАТАЦИИ:

- По едно от изискванията за управление на активите, относно това дали информацията, която съдържа описа е еднозначна информация (чл.8, ал.2) всичките 5 общини от първа категория за декларирали, че го спазват. На другите две изисквания, 4 общини са дали положителен отговор.

- При общините втора категория 4 общини са отговорили положително на третото изискване, относно това дали информацията, която съдържа описа е еднозначна информация на 3 общини - на другите две изисквания. Аналогична е бройката на общините трета категория които отговарят на различните изисквания по чл.8, ал.2 от НМИМИС.

- Базирайки се на примери от съществуващата си добра практика, екипът счита, че в тази част от анализа следва да се обърне внимание на един обективно съществуващ проблем свързан с управление на информационните активи. Проблемата се отнася до ИКС до приложения или до решения, разработени или приети в рамките на общините, но извън своята формална, обикновено централизирана ИКТ структура. Те са в резултат от това, че потребителите се опитват да решат практически проблем с инструменти, които се предлагат на пазара на ниска цена или безплатно, когато решенията, предоставени от установените канали и чрез ИТ звената, може да се счита, че не отговаря на разполагаемите от тях време, разходи или изисквания за персонализиране. Също може да бъдат резултат от желание за бързо нововъведение в лицето на променящите се изисквания или за осигуряване на съвместимост с инструменти използвани от партньорите по изпълнението на определени дейности и които може да се различават от решения, одобрени от общината. Примери за това са създаването безплатни акаунти при доставчици на услуги, предлагащи софтуерни решения съхранение на данни, прехвърляне на файлове, уеб дизайн или управление на съдържание, или разработка на вътрешни приложения за индивидуално използване или проекти. Тези решения обикновено не се проверяват или не винаги се проверяват за съответствие с изискванията и процедурите по МИС съществуващи в общината т.е следователно би могло до се счита , че работят в „сенчеста среда“.

ИЗВОДИ:

- Посочените от общините данни дават повод да се предположи, че управлението на активите е една от дейностите, при която повечето общини са приложили мерки съответстващи на изискванията на НМИМИС.

- Възможни са проблеми за МИС породени от наличието (за общините където има такива) на пропуски в тази дейност.

- Екипът смята, че проблемите с МИС, свързани с използване на ИТ „в сянка“, изискват повече внимание при балансиране необходимостта от контрол в среда, изложена на кибер рискове и оправдава цели и конструктивна мотивация на потребителите за иновации, и използване на алтернативни решения, когато има такива.

- В тази връзка и подхода към такива сенчести ИТ решения следва да бъде добре балансиран тъй като може да се предположи, че желанието на някои потребители използвайки такива решения, е здравословен знак за готовност за иновации, за което структурните звена обикновено трябва да имат определени ресурси и свобода на действие, и които в повечето случаи са недостатъчни.

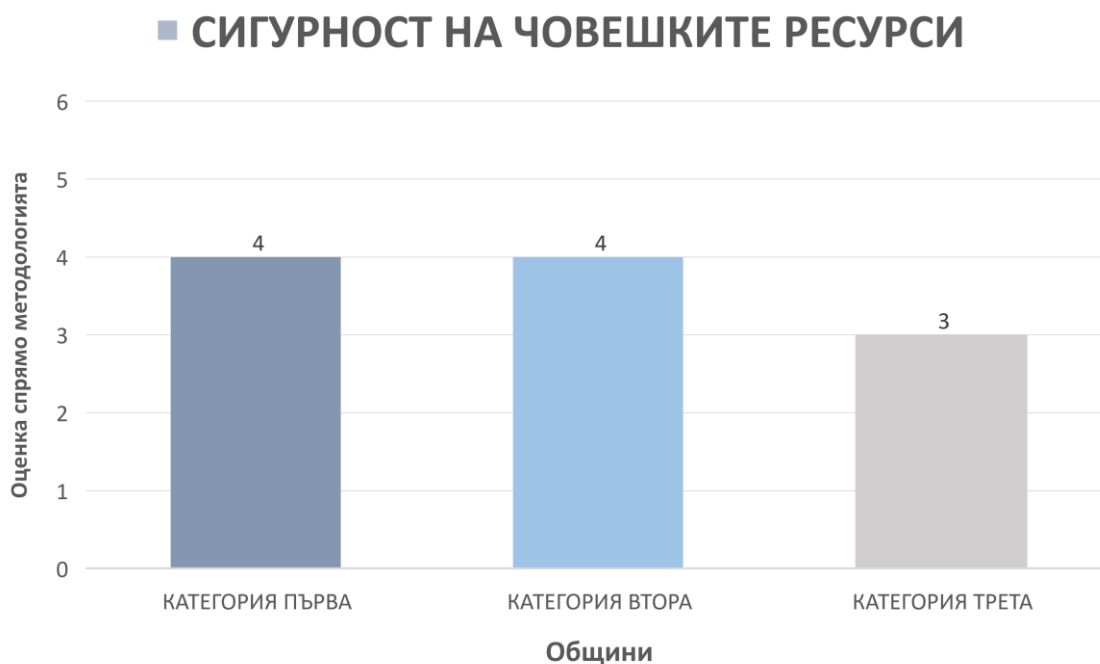
ПРЕПОРЪКИ.

- Ръководителите на 7 –те общини от трите категории (2 от първа категория, 2 от втора категория и 3 от трета категория) имащи пропуски в дейността си по управление на активите да организират отстраняването им. Дейността е свързана изцяло с организационни мерки.

- По отношение например на сенчестите ИТ решения могат да бъдат приети следните идеи: създаване или разширяване на безопасна среда позволяваща тестване и прилагане на цифрови иновации; насочване на вниманието към развитието на разпределени ИКТ в по-децентрализирана среда с участие на щатните ИТ служители; както и подобряване на обучението на евентуални потребители, предприемане на мерки за повишаване на осведомеността за получаване на надеждна и ясна информация при използването на такива решения.

8. Сигурност на човешките ресурси

Резултати:



Фигура 7 Резултати от проведено проучване по т. Сигурност на човешките ресурси.

КОНСТАТАЦИИ:

- Първите пет изисквания от чл.9, ал.2 (отнасящи се преди всичко до обезпечаване на МИС в процесите по подбор, назначаване, преназначаване, на служители) се изпълняват от 4 общини първа категория. Останалите две изисквания от същия чл. на НМИМИС относно обезпечаването на професионално обучение и на провеждането на ежегоден инструктаж за повишаване на осведомеността се изпълняват от две общини.

- За общините втора категория бройката, е аналогична – 4 на 2.

- Малко по-различна е картината при общините трета категория. Там ежегоден инструктаж за повишаване на осведомеността по МИС, провежда само една община. Две общини са документирали задълженията на лицата по МИС, с ясно и точно отразяване в длъжностните им характеристики.

- За провеждане на обучение в съответствие с изискванията на чл.9, ал.4, т.1 от НМИМИС се използват преди всичко възможностите които предоставя за тази цел Института за публична администрация и различни други безплатни обучения.

- Задължително условие за високо ниво на МИС в общините несъмнено е наличието на високоподготвени и силно мотивирани ИТ служители и най-вече на служители по МИС И това разбира се е отправна точка, която екипът счита ,че не подлежи на съмнение. Възможността за работа в цифрова среда вече не е въпрос на избор от отделния служител, а обективна реалност. Свободно използване на стандартно електронно оборудване и приложения са абсолютно необходими за всеки потребител на цифровата инфраструктура на общината. При изпълнение на това основно изискване, следва да се взисква от служителите, да спазват и мерките за МИС.

- Задължително е да се направи и по-сериозно усилие от повишаване на осведомеността за правилата, отговорностите и средствата по МИС, за постигане на трайна промяна в поведението и промяна в подхода към МИС.

- Освен от технологична готовност, свързана с цифровизиране на общоадминистративни и специализирани дейности в общините, МИС следва да е резултат от многостранен подход.Подходът трябва да обхваща всички нива на оцината, включително органи за вземане на решен ия и управление, надзорни органи, изпълнително ръководство, оперативно или функционални структурни звена, програмни мениджъри, персонала като цяло и външни доставчици на услуги. С други думи, за да се създадат условия за повишаването на кибер устойчивостта се изисква цялостен организационен подход. Освен това МИС засяга няколко организационни области и компетенции, включително ИКТ, управление на риска, физическа сигурност и защита, и управление на информация и знания в по-широк план.

- Както вече беше споменато по-горе от особено важно значение е повишаване на киберкултурата, което е свързано преди всичко с другите категории служители.

- Две от общините от първа категория, 3 общини от 2 категория и 2 общини от 3 категории извършват периодически задължително обучение за повишаване на квалификацията в съответствие с използваните техника и технологии.

- На някои потребители по обективни причини са налага поради ограничените ресурси да използват личните си устройства за влизане в ресурси на общините. Такива служители , потребители на системи и инфраструктура в общините е по-малко вероятно да бъдат информирани за правилната и безопасна употреба в съответствие с приложимите разпоредби и практики в общината. Тези проблеми може допълнително да се изостри в общините, където има евентуално висок дял служители консултанти, изпълнители и краткотросочно нает персонал. В тази връзка Роководството на общини следва да има предвид, че инициативите за обучение и повишаване на осведомеността трябва обхващат целия персонал. Заплахите не правят разлика между различните потребителски категории.

ИЗВОДИ:

- Необосновано в по-голямата част от общините са подценени въпросите с - инструктажи за повишаване на осведомеността по отношение на МИС

- Първата стъпка към повишаването на професионалната квалификация на служителите в съответствие с използваната техника и за изграждането на професионална култура на киберсигурност е осведоменост на ръководство на общината за свързаните рискове и с развитие на разбиране за последствия от ниска квалификация и от лоша киберхигиена, на служителите.

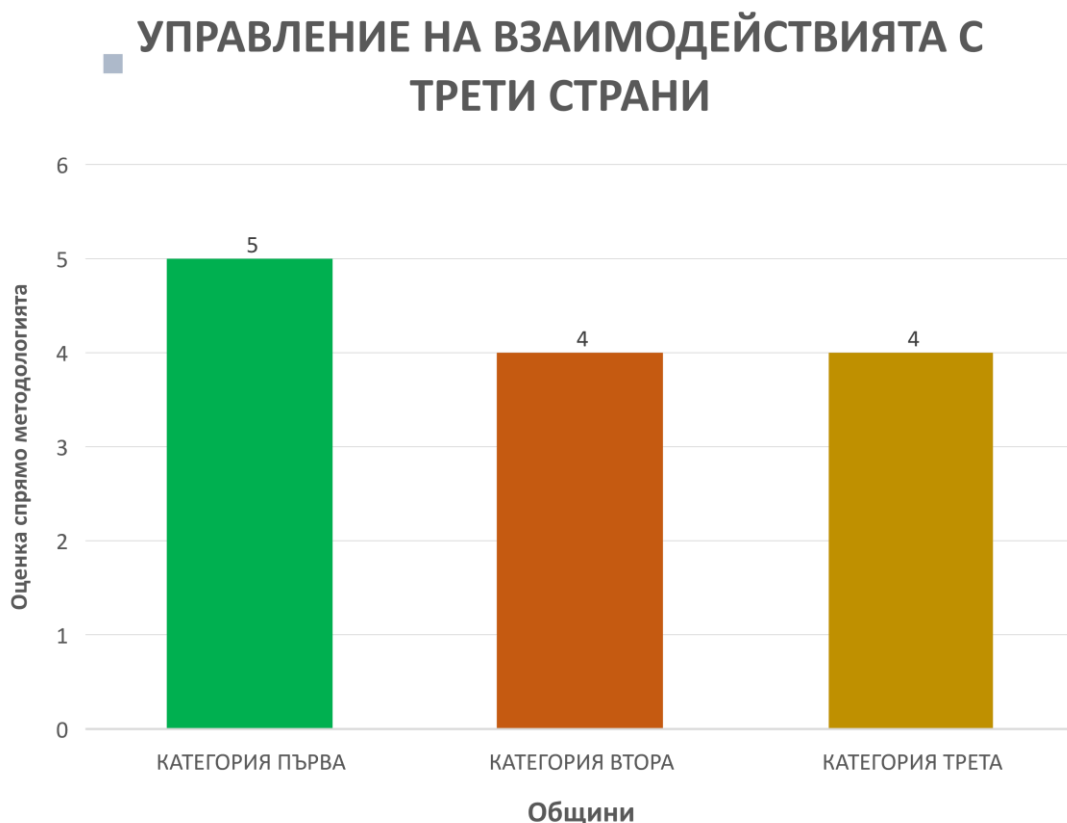
- Това предполага активна позиция от ръководството, която иска да се създадат такива механизми за вътрешно управление, което да им дава необходимата информация и фактическа база. В това отношение ролята на лидерството надхвърля вземане на решения относно разпределението на ресурсите. Ключът тук е насърчаване повишаването на професионалната квалификация и на киберкултурата, при която разпознаването и активното наблюдение на възникването инциденти се възприема не като признание за провал, а като отправна точка за съвместно решаване на общ проблем и укрепване защитата на общината и нейните ресурси. Други начини, по които ръководството може да стимулира действие и по конкретно да повлияе на начина на мислене в цялата система на подчинение - да показват модел на препоръчително поведение, да дават управленски отчетност в цялата организация, участие в програми за подобряване информираност и демонстриране на активен стил на лидерство по въпросите на МИС като цяло.

ПРЕПОРЪКА:

- Екипът препоръчва ръководители на онези общини, които не са обезпечили повишаване на професионална квалификация и не са предприели провеждането на инструктаж да предприемат необходимите мерки за изпълнението на изискванията.

9. Управление на взаимодействията с трети страни

Резултати:



Фигура 8 Резултати от проведено проучване по т. Управление на взаимодействията с трети страни.

КОНСТАТАЦИИ:

- Четири от общините първа категория са изпълнили 6 (от общо 8) от изискванията за МИС при взаимоотношенията с трети страни.

- Четири общини втора категория са изпълнили 7 от изискванията

- Една община трета категория е изпълнила 6 от изискванията, други три общини са изпълнили 3 от изискванията.

- Преобладаваща част от общините трета категория изпълняват изискванията за включване в договорите с доставчици клаузи за МИС, свързани с негов достъп до активи на общините и на изискването за определяне на отговорник следящ за спазване на изискванията по договорите.

- На европейско и национално ниво нараства и вниманието, което се отделя на взаимоотношенията с трети страни в областта на МИС. Като пример могат да се споменат повсеместните проверки в държавите членки на ЕС за сигурността на основни компоненти от 5G мобилни мрежи, които са произведени в Китай, обръщането на специално внимание за сигурността на веригите за доставка в Директива 2022/2555 (ДМИС2), наличието на специални текстове относно веригите за доставки в проекта на Cyber Resilience act (Закон за киберустойчивост) и , който е в процес на приемане в рамките на ЕС и който най-общо казано се предвижда да въведе изисквания за ИТсмарт устройствата да притежават сертификат за МИС.

- В тази насока от най-важно значение са отношенията с доставчици на услуги в областите на МИС и на ИКС. Общо взето на практика функционират три варианта за поддържане на ИКС и на МИС – със собствени служители, с доставчици на външни услуги за сигурност чрез договорни отношения или хибридни решения. Участващите общини имат различни гледни точки за . предимства и недостатъци на вътрешните решения спрямо външните.

ИЗВОДИ:

- При общини които използват хибридни решения, като правило се разграничават стратегически и надзорни функции които от една страна, остават в правомощията на общините и текущи дейности които се прехвърлят на външни доставчици на такива услуги.

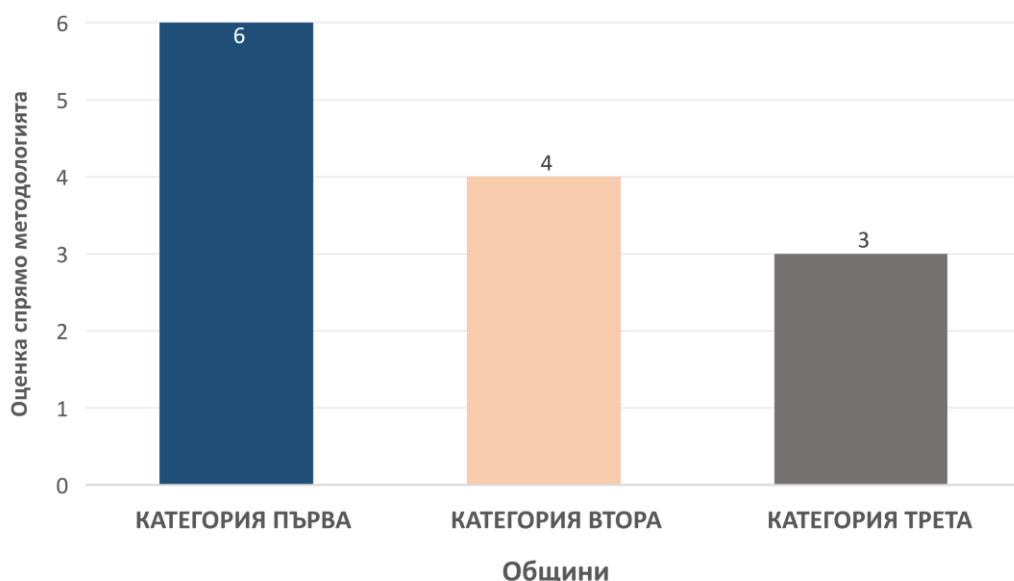
ПРЕПОРЪКИ:

- Екипът препоръчва на ръководствата на общини да бъдат много внимателни и прецизни при взаимоотношенията си с трети страни и безусловно да прилагат всички изисквания по МИС предвидени в Наредбата в тази и част.

10. Управление на измененията в информационните активи

Резултати:

УПРАВЛЕНИЕ НА ИЗМЕНЕНИЯТА В ИНФОРМАЦИОННИТЕ АКТИВИ



Фигура 9 Резултати от проведено проучване по т. Управление на измененията на информационните активи.

КОНСТАТАЦИИ:

- Всички общини от първа категория са изпълнили 5 (от общо 8) от изискванията на Наредбата по чл.11. „Управление на измененията на информационните активи“. Две общини не са приложили мерки за изпълнение на изискването за наличието на одобрен план за управление на изменения в информационните активи и при извършване на оценка на риска при тези изменения.

- На 6 (от общо 8) от изискванията отговарят 3 от общините втора категория. Две общини не изпълняват нито едно от изискванията по чл.11 от Наредбата.

- Най-пъстра е картината при общините трета категория. На 5 от изискванията, отговарят 5 общини, на 2 изисквания отговарят 4 общини. Две общини не отговарят на нито едно изискване за управление измененията на информационните активи.

ИЗВОДИ:

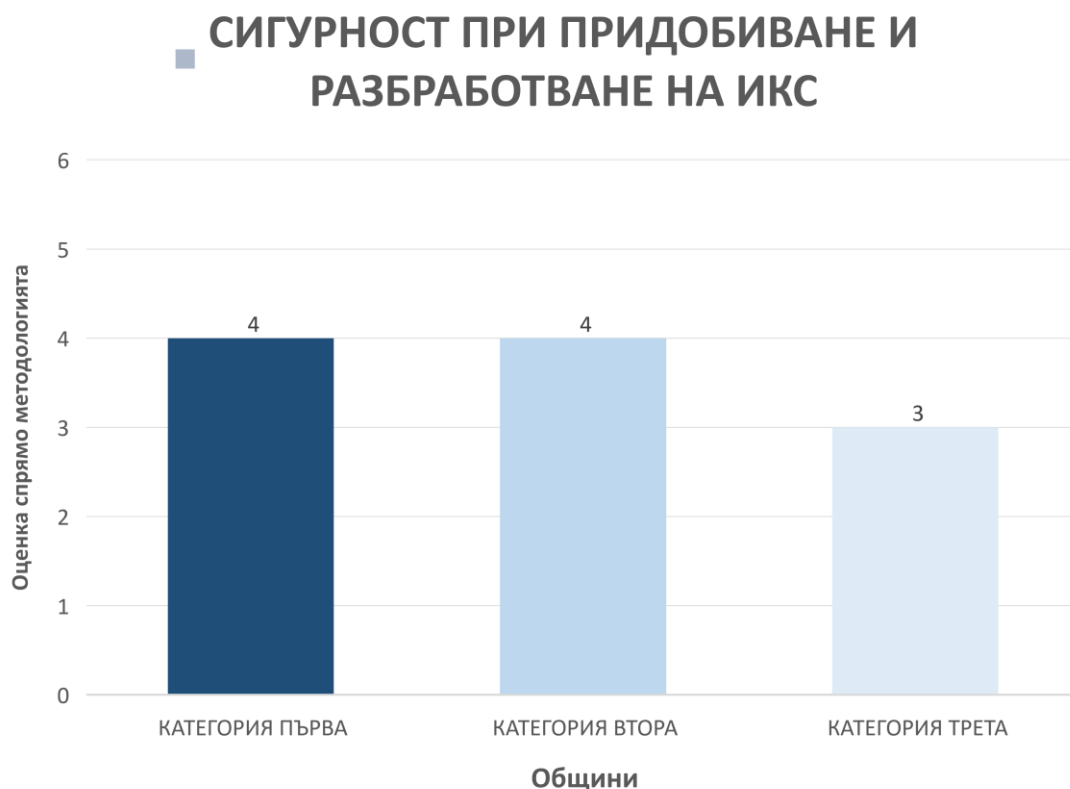
- Спазване на изискванията за МИС при управление изменението на активи, е приоритетно и отлично организирано при общините първа категория, добре – при общините втора категория и удовлетворително при общините трета категория.

ПРЕПОРЪКИ:

- Ръководителите на общини втора и трета категория които не са изпълнили всички или по-голямата част от изисквания за МИС при управление изменението в активите да предприемат организационни мерки за промяна статуса на това състояние.

11. Сигурност при придобиване и разработване на ИКС

Резултати:



Фигура 10 Резултати от проведено проучване по т. Сигурност при придобиване и разработване на ИКС.

КОНСТАТАЦИИ:

- Четри от общините първа категория, въвеждат в експлоатация ИКС, след успешно проведени и документиращи тестове, доказващи защита на информацията, а една от общините не изпълнява това изискване.

- Три от общините от втора категория въвеждат в експлоатация ИКС след тестове, а две не провеждат такива тестове.

- Само две общини трета категория провеждат тестове при въвеждането в експлоатация на нови ИКС, а 4 не провеждат тестове.

- В съответствие с разбиране, че в процеса на разработване и придобиване на ИКС отговорността за МИС не е отговорност само на ИТ звената, то отговорности имат и структурните звена, както в общата администрация, включително звено „Обществени поръчки“, така и в други структурни звена от администрацията. Информацията, събрана по време на изследването, навежда на мисълта, че в част от структурните звена на общините, като, че ли не се приемат достатъчно сериозно въпросите на МИС поради което и не се вземат предвид изискванията за МИС и устойчивост при разработването и изпълнението на съответните проекти и дейности.

ИЗВОДИ:

- Включването на изискванията за МИС следва да бъде неотменна част в етапите на разработване и внедряване на ИКС. Заедно с успешно провеждане и документиране на тестове при въвеждане в експлоатация на тези ИКС ще се приложи и принципа „security by design“, т.е. изискванията за МИС ще се планират и осигурят от самото начало на жизнения цикъл на ИКС, а няма да се добавят впоследствие.

ПРЕПОРЪКИ:

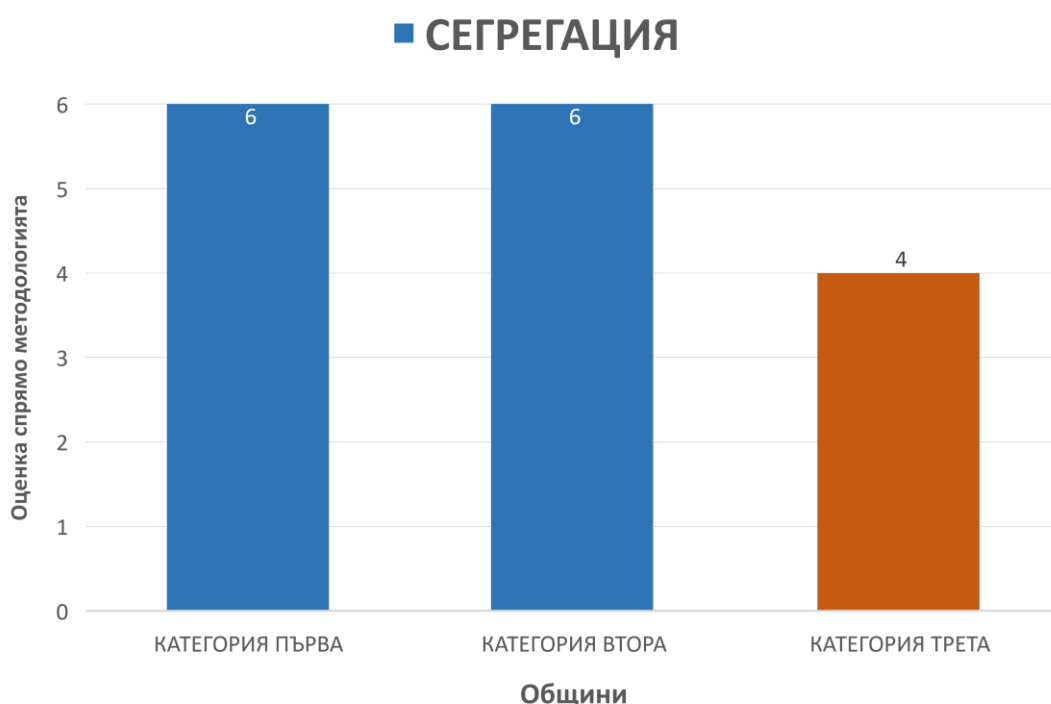
- Да се прилагат ясни изисквания по МИС, при изпълнение на административните функции в процеса на проектиране и въвеждане в експлоатация на ИКС Това може да намали непълнотите във функционалните характеристики на различните структурни звена в общините и на липсата на участието на някои от тях в този процес.

- Интегриране на изискванията за МИС в политиката и практиката при проектиране и изграждане на ИКС във всички звена само по себе си ще бъде признание, че такъв подход конструктивно допринесе за постигането на цялостен организационен подход в общината по този въпрос.

РАЗДЕЛ II – ЗАЩИТА

12. Сегрегация

Резултати:



Фигура 11 Резултати от проведено проучване по т. Сегрегация.

КОНСТАТАЦИИ:

- Всички общини първа и втора категория изпълняват изискванията по чл.13 от НМИМИС, отнасящи се до разделяне и изолиране помежду им на ИКС изпълняващи различни функции.

- Половината (3 бр.) от общините трета категория са декларирали, че отговарят на тези изисквания.

ИЗВОДИ:

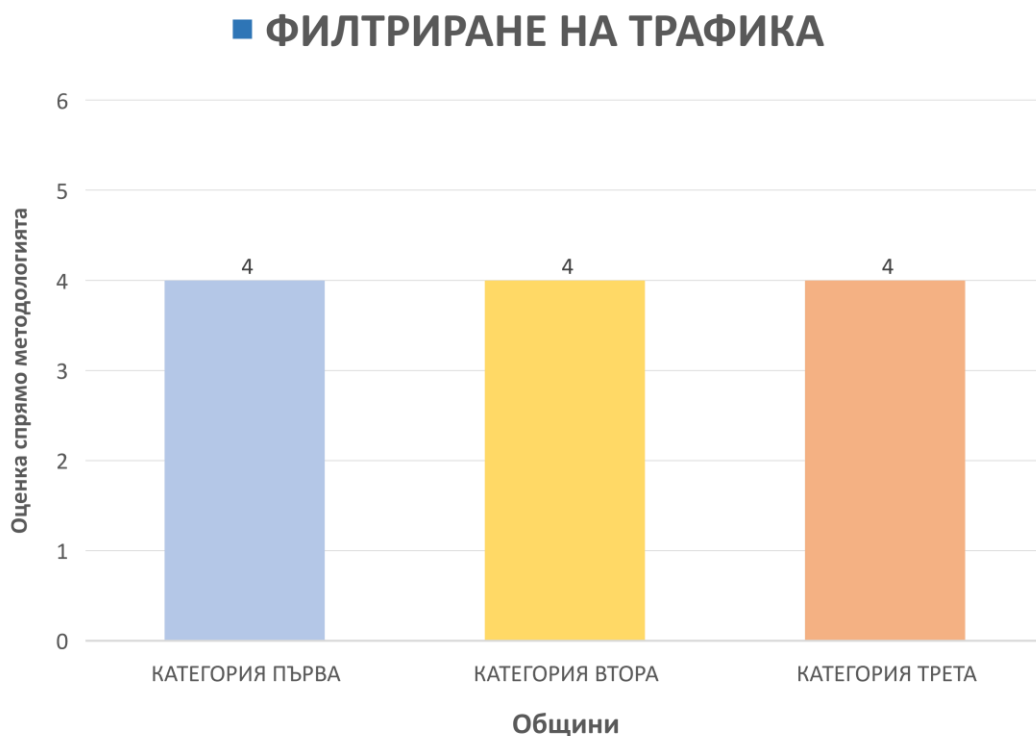
- Преобладаваща част от общините са предприели необходимите мерки за изпълнение на изискванията по чл.13 от Наредбата.

ПРЕПОРЪКИ:

- Ръководствата на общините от трета категория, които не са осигурили разделяне и изолиране помежду им на ИКС изпълняващи различни функции да предприемат мерки за разделянето им.

13. Филтриране на трафика

Резултати:



Фигура 12 Резултати от проведено проучване по т. Филтриране на трафика.

КОНСТАТАЦИИ:

- Правила за филтриране на трафика са разработили по 3 общини от трите категории.
- Ненужните портове по протоколи TCP и UDP, са затворени от всички общини първа категория, от 4 общини втора категория и 5 общини трета категория.

ИЗВОДИ:

- Изследваните общини частично спазват правила за филтриране на трафика.
- Значително по-голям брой общини (14 бр.), са затворили ненужните портове по посочените по-горе протоколи.

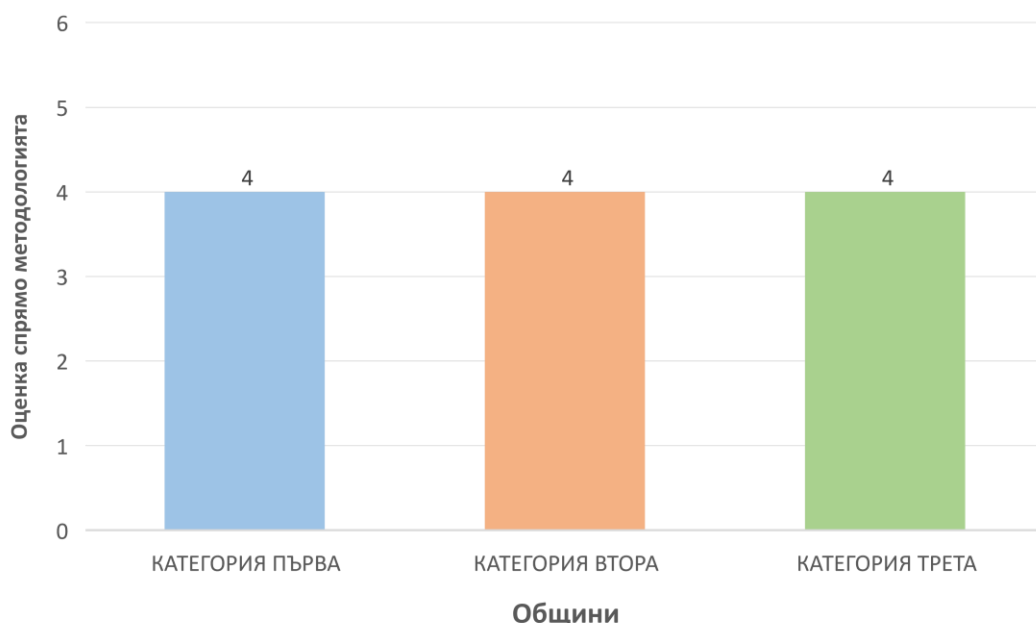
ПРЕПОРЪКИ:

- Ръководствата на общини, които нямат Правила за филтриране на трафика, да предприемат мерки за разработване и прилагане на такива правила.
- Екипът настоятелно препоръчва ръководствата на двете общини в които не са затворени ненужните портове по протоколи TCP и UDP да вземт незабавни мерки за затварянето им.

14. Неоторизирано използване на устройството

Резултати:

НЕОТОРИЗИРАНО ИЗПОЛЗВАНЕ НА УСТРОЙСТВОТО



Фигура 13 Резултати от проведено проучване по т. Неоторизирано използване на устройството.

КОНСТАТАЦИИ:

- Политика за използване на лични технически средства и преносими записващи устройства са разработили и прилагат 4 общини от първа категория, 3 от втора категория и 4 от трета категория.

ИЗВОДИ:

- По-голямата част (11 бр.) от общините са осъзнали необходимостта от регламентиране използването на лични технически средства и преносими записващи устройства, като са регламентирали тези дейности.

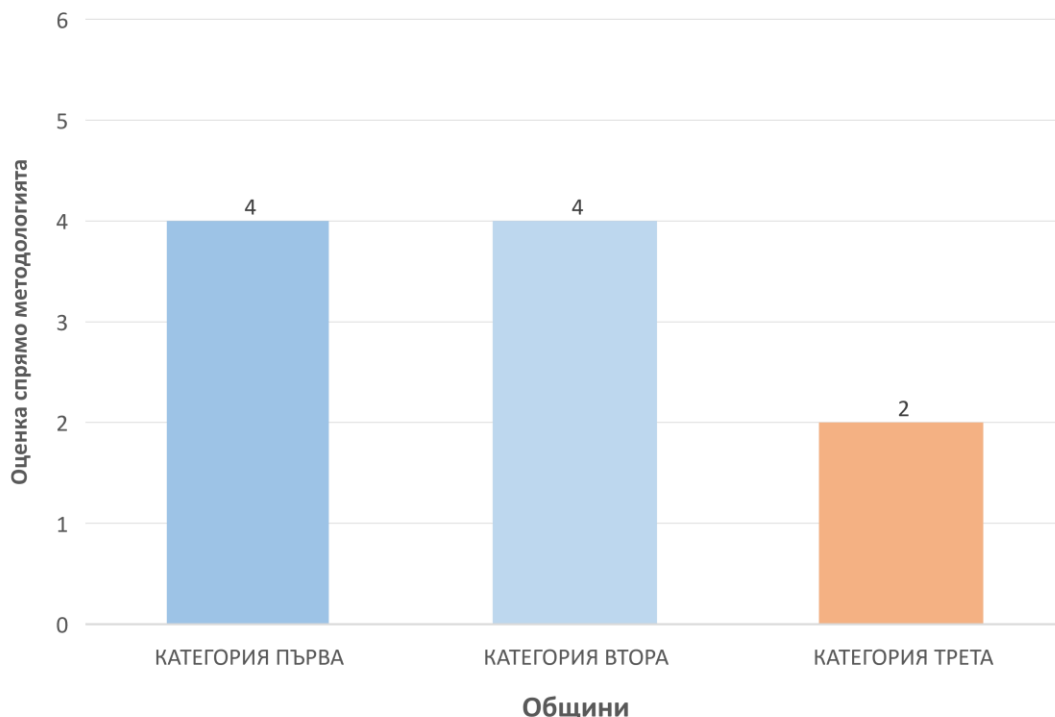
ПРЕПОРЪКИ:

- С цел намаляване на рисковете от несанкциониран достъп до информационните активи на общините, екипът препоръчва на Ръководствата на 5-те общини, които не са регламентирали горепосочените дейности да предприемат организационни мерки за създаването на политика за използването на лични технически средства и записващи устройства.

15. Криптография

Резултати:

■ КРИПТОГРАФИЯ



Фигура 14 Резултати от проведено проучване по т. Криптография.

КОНСТАТАЦИИ:

- Политика и вътрешни правила за прилагане на криптографски механизми са разработили и приложили по 4бр. общини от първа и втора категория и само една община от трета категория.

ИЗВОДИ:

- Необходимостта от използването на криптографски механизми за гарантиране на конфиденциалността и интегритета на чувствителна информация е приоритетна и реализирана цел в дейностите на 9 общини. Останалите 7 общини недоценяват тази необходимост.

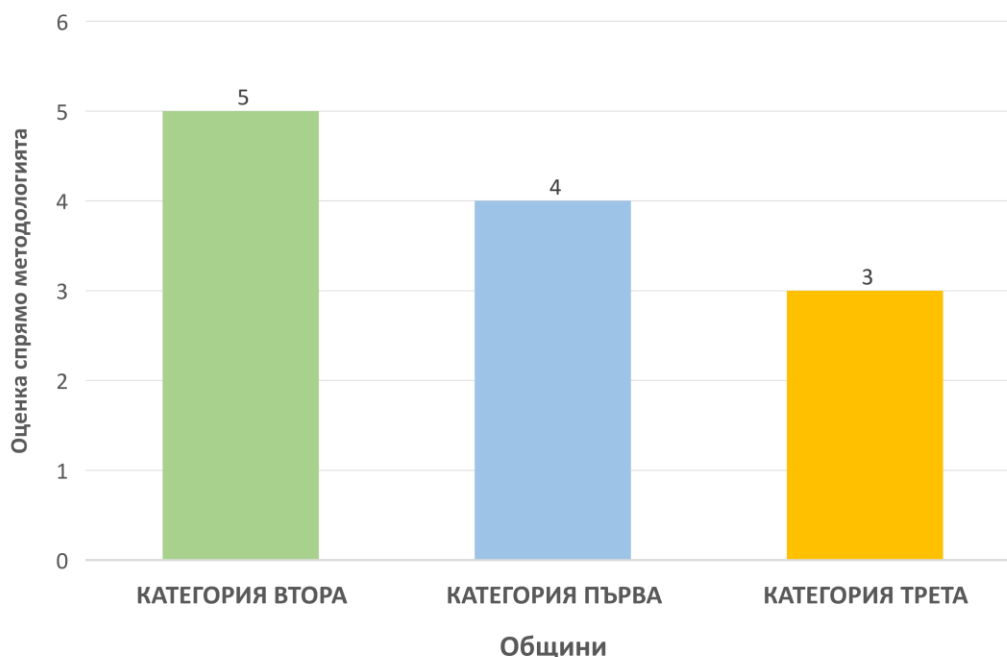
ПРЕПОРЪКИ:

- Екипът препоръчва на Ръководствата на 7-те общини в които няма политика за използване на криптографски механизми с цел да осигурят гарантиране конфиденциалността и интегритета на чувствителна информация и съобразена с уязвимостта на информацията, да предприемат мерки за разработване и прилагане на такава политика.

16. Администриране на ИКС;

Резултати 15

■ АДМИНИСТРИРАНЕ НА ИКС

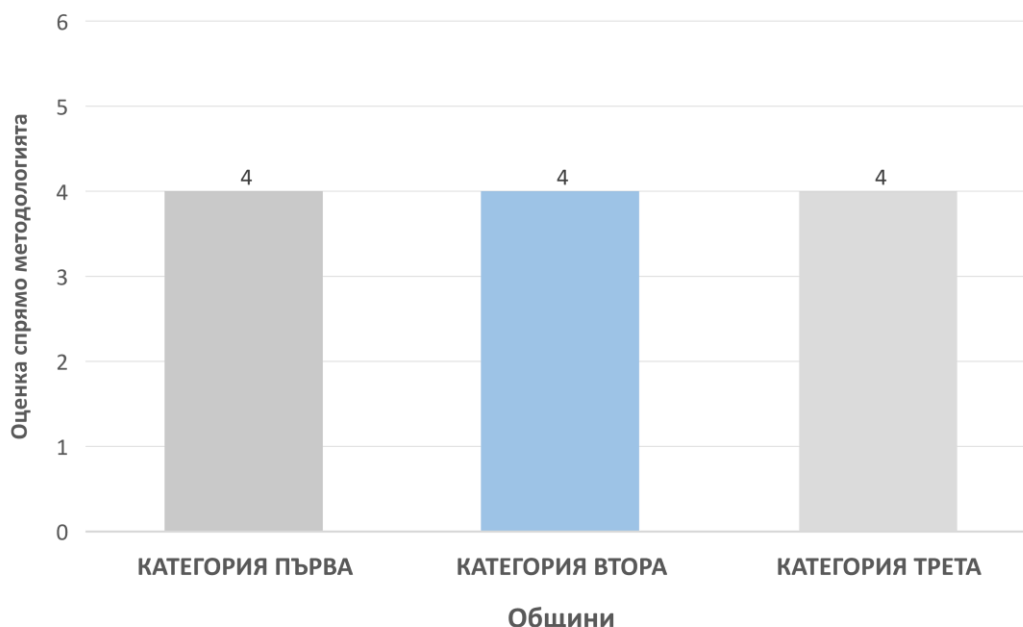


Фигура 15 резултати от проведено проучване по т. Администриране на ИКС

17. Среда за администриране

Резултати 16

■ СРЕДА ЗА АДМИНИСТРИРАНЕ



Фигура 16 Резултати от проведено проучване по т. Среда за администриране.

КОНСТАТАЦИИ:

- Пет от изискванията (от всичко 12) свързани с администриране на ИКС по чл.17 „Администриране на ИКС“ от НМИМИС се прилагат от всички общини първа категория, 3

Проект BG05SFOP001-2.025-0133 „Повишаване на общото ниво на мрежова и информационна сигурност в общинските администрации“ се реализира с финансовата подкрепа на Оперативна програма „Добро управление“ 2014-2020, съфинансирана от Европейския съюз чрез Европейския социален фонд

Project BG05SFOP001-2.025-0133 “Increasing the overall level of network and information security in municipal administrations” is implemented with the financial support of the Operational Programme “Good Governance” 2014-2020, co-financed by the European Union through the European Social Fund

изисквания – от по 4 общини, 2 изисквания от по 2 общини, 1 изискване от по 2 общини и 2 изисквания от нито една община.

- Всички общините втора категория са изпълнили 8 от изискванията на чл.17 от НМИМИС, 3 от изискванията са изпълнили 2 общини, 2 от изискванията са изпълнили 2 общини и 1 изискване е изпълнено от само една община.

- Нито една община от трета категория не е изпълнила всички изисквания при администрирането на ИКС. 1 изискване е изпълнено от 5 общини, 4 изисквания са изпълнени от 4 общини, 3 изисквания – от 3 общини, 4 изисквания – от 2 общини и 1 изискване не е изпълнено от нито една община.

- По три общини от трите категории са изпълнили изискванията по чл.18 „Среда за администриране“

ИЗВОДИ:

- Ръководствата на почти всички общини втора категория са приоритизирали на висока степен въпросите по администриране на ИКС, в резултат, на което е постигната значителна защита на профилите с административни правила. Своевременно се сменят паролите за автентификация, всички операции, процеси и дейности в ИКС се документира, като в тази документация не се съхраняват пароли в явен текст или хеш.

Голяма част от Ръководителите на общини първ категория също са предприели подобни адекватни мерки.

- При общините трета категория обаче ръководителите осигурили прилагането на мерки за изпълнение на изискванията за администриране на ИКС, както и на необходимата среда за администриране са малцинство, което показва че там се пренебрегва в някаква степен необходимостта от администриране на ИКС съобразено изискванията на НМИМИС.

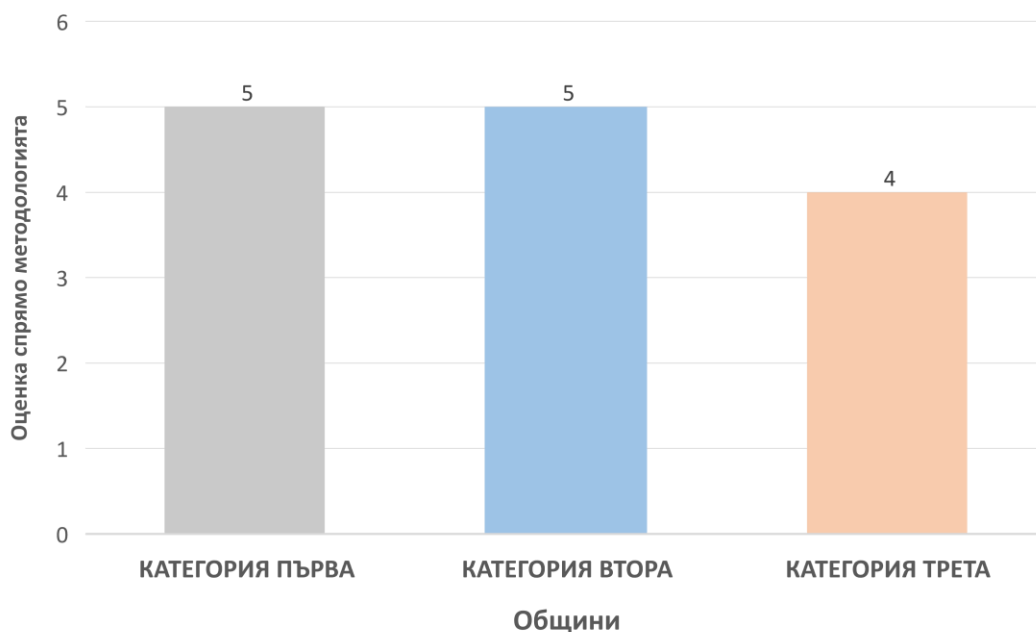
ПРЕПОРЪКИ:

- Доколкото имплементирането на повечето от неизпълнените изисквания е свързано преди всичко с организационни мерки, екипът препоръчва на Ръководителите на общините неотговарящи на едно или повече от изискванията да предприемат мерки за прилагането им.

18. Управление на достъпите

Резултати:

■ УПРАВЛЕНИЕ НА ДОСТЪПИТЕ

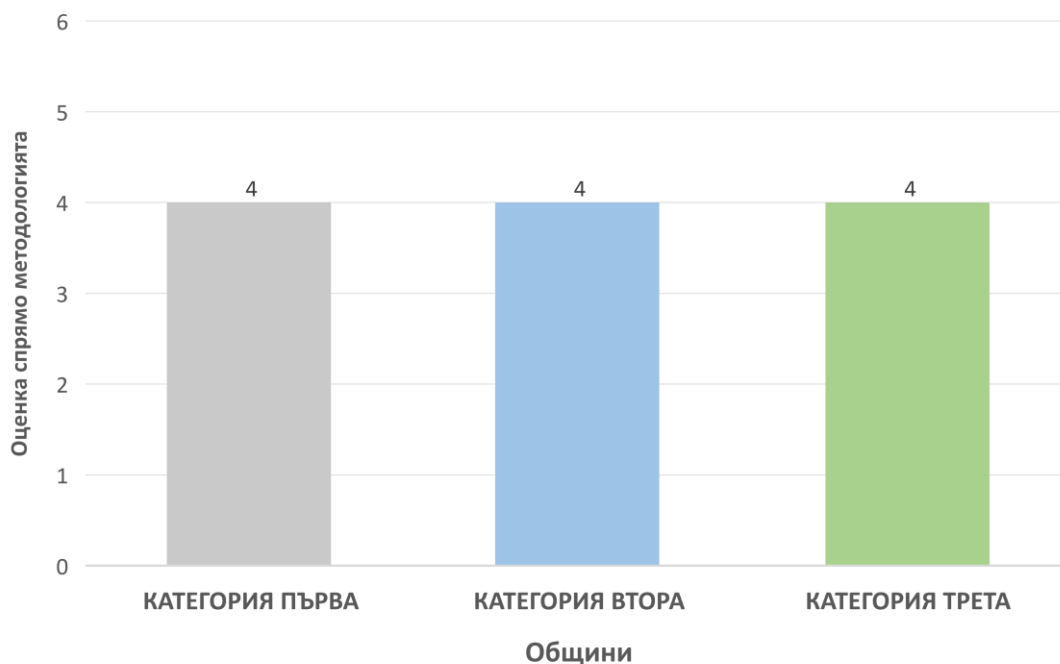


Фигура 17 Резултати от проведено проучване по т. Управление на достъпите.

19. Защита при отдалечен достъп*

Резултати:

■ ЗАЩИТА ПРИ ОТДАЛЕЧЕН ДОСТЪП



Фигура 18 Резултати от проведено проучване по т. Защита при отдалечен достъп.

КОНСТАТАЦИИ:

Проект BG05SFOP001-2.025-0133 „Повишаване на общото ниво на мрежова и информационна сигурност в общинските администрации“ се реализира с финансовата подкрепа на Оперативна програма „Добро управление“ 2014-2020, съфинансирана от Европейския съюз чрез Европейския социален фонд

Project BG05SFOP001-2.025-0133 “Increasing the overall level of network and information security in municipal administrations” is implemented with the financial support of the Operational Programme “Good Governance” 2014-2020, co-financed by the European Union through the European Social Fund

- С изключение на едно от изискванията по чл.19. „Управление на достъпите“ всички общини от първа категория отговарят на останалите изисквания. Осигурен е достъп до ИКС на потребител или автоматизиран процес само когато това е строго необходимо за изпълнение на служебни задължения; създадени са и се прилагат вътрешни правила по т.1 от чл.19, отнасящи се до даване на достъп до конкретни информационни активи на служителите според заеманата длъжност, ограничава се привилегироваността на определени лица само за определен период, през който период се контрол действията с него, достъпът да споделени файлове и принтери се извършва само по контролирана мрежа.

- Едно от изискванията се изпълнява от всички общини от втора категория, останалите изисквания се изпълняват от 4 бр. общини.

- Четири от изискванията се изпълняват от 3 общини, а 4 общини изпълняват 3 изисквания.

- По три от трите категории общини изпълняват изискванията по чл.20 „Защита при отдалечен достъп“, отнасящи се до –използването на двуфакторна автентификация, използването само на канали с висока степен на защита VPN, като не се използват File Transfer Protocol и Remote Desktop Connection.

ИЗВОДИ:

- В общините от втора и в по-малка степен от първа категория са създадени условия и се прилагат изискванията за управление на достъпите.

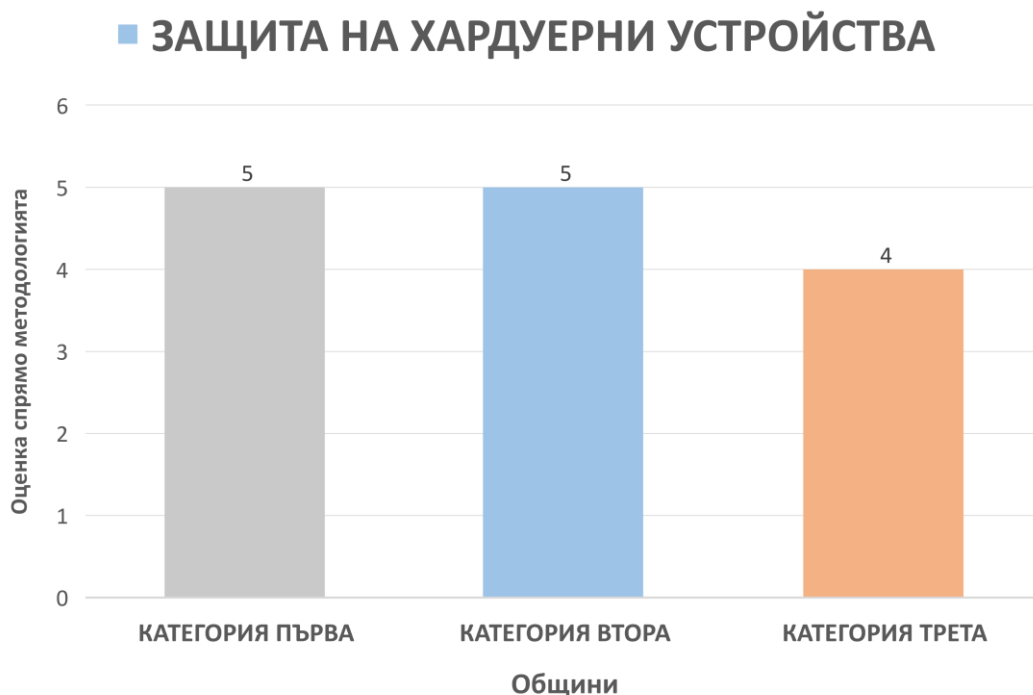
- В някои от общините трета категория този въпрос е недооценен, което е препоставка за киберинциденти.

ПРЕПОРЪКИ:

- Предвид характера на мярките които следва да се предприемат за управление на достъпите, както и реалната заплаха за МИС на ИКС там където не са приложени, екипът препоръчва да се приложат адекватни и пропорционални мерки за спазване изискванията на чл.19.

20. Защита на хардуерни устройства

Резултати:



Фигура 19 Резултати от проведено проучване по т. Защита на хардуерни устройства.

КОНСТАТАЦИИ:

- Изискванията за защита на хардуерните устройства се изпълняват изцяло от почти всички общини първа и втора категория. Създадени се необходимите климатично-механични условия за хардуерните устройства и се наблюдават параметрите на тези условия да бъдат в съответствие с препоръките на производителя. В съответствие с информацията с която работят устройствата са разположени във физически защитена зони.

- Две общини трета категория отговарят на 10 (от общо 12) изисквания, 2 общини изпълняват 6 от изискванията, 1 община не изпълнява нито едно изискване.

ИЗВОДИ:

- В общините първа и втора категория изискванията за защита на хардуерните устройства се изпълняват във висока степен.

- По-малко от половината общини трета категория защитават хардуерните устройства във висока степен. Налице е неприемлив риск за състоянието на МИС, в останалите общини от тази категории.

ПРЕПОРЪКИ:

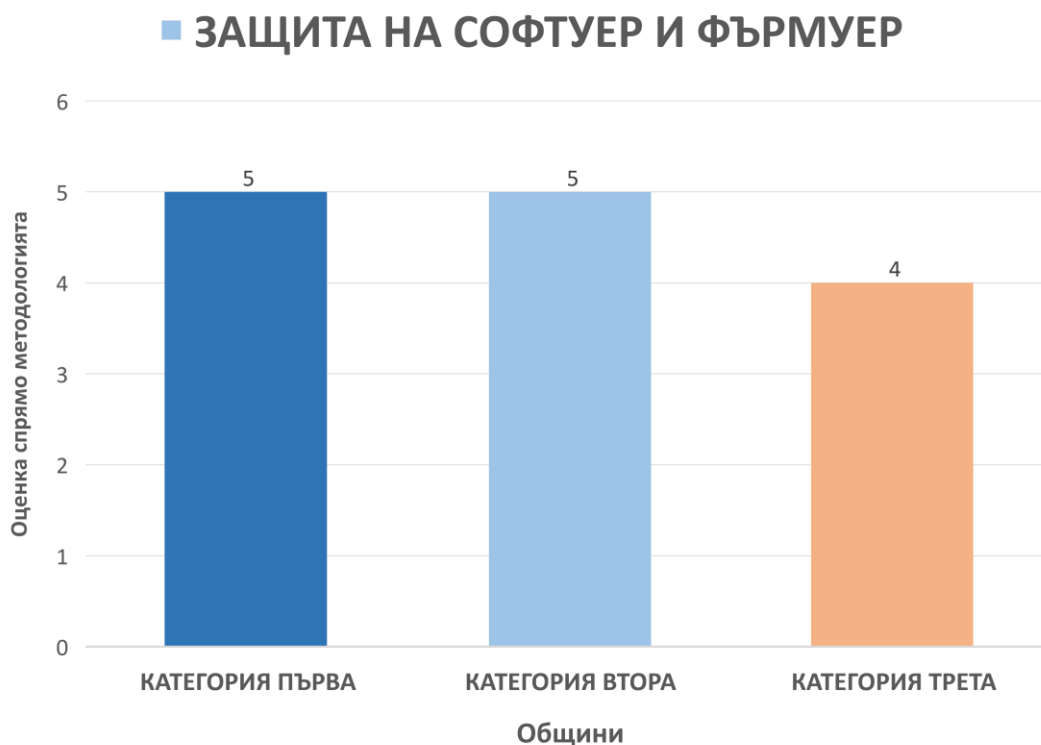
- Предвид гореизложеното, екипът препоръчва на ръководствата на общини първа втора категория да продължат да прилагат мерките изискуеми за защита на хардуерните устройства.

- На ръководителите на общини трета категория, които не са изпълнили частично или цялостно тези изисквания, екипът препоръчва да предприемат необходимите мерки с цел да се осигурят препоръчаните физико механични условия за работа на ИКС.

- Като възможна мярка екипът, препоръчва да се установят контакти с Министерство на електронното управление с цел използване ресурса на Държавния хибриден и частен облак в интерес на общините.

21. Защита на софтуер и фърмуер

Резултати:

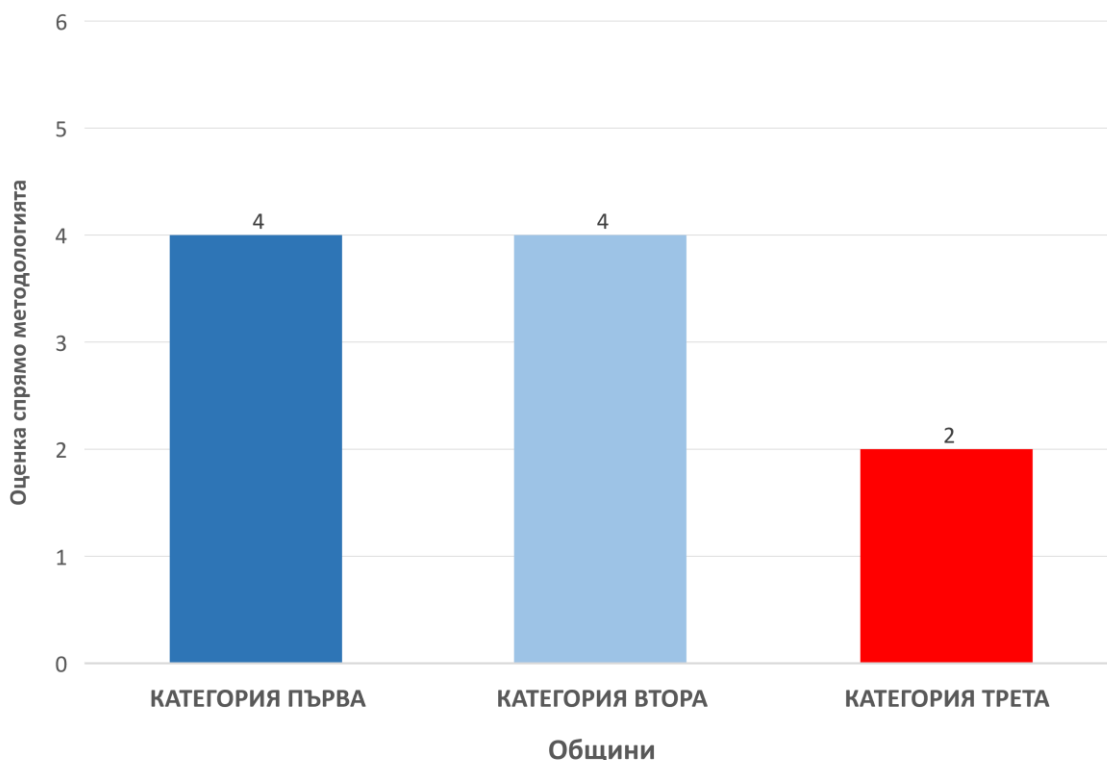


Фигура 20 Резултати от проведено проучване по т. Защита на софтуер и фърмуер.

22. Изисквания за конфигуриране*

Резултати:

■ ИЗИСКВАНИЯ ЗА КОНФИГУРИРАНЕ



Фигура 21 Резултати от проведено проучване по т. Изисквания за конфигуриране.

КОНСТАТАЦИИ:

1) Защита на софтуер и фърмуер

- Четри от общините първа категория спазват почти всички изисквания по чл.21. „Защита на софтуер и фърмуер“ и отнасящи се преди всичко до използването само на актуален софтуер и фърмуер поддържан от производителите, до наличие на списък с одобрен софтуер който се използва в общината, наличие на библиотека с дистрибутиви на използвания софтуер, наличие на правила и инструкции за достъп до нея, до недопускането за използване на неodobрен софтуер, до наличие на правила за управление на уязвимости, до наличие на актуални off line копия на актуалните конфигурационни файлове и/или описание на настройките, регулярна проверка състоянието на конфигурационните файлове.

- Над половината (Збр.) от общините втора категория отговарят на тези изисквания.

- Многообразна е картината при общини от трета категория, като различен брой общини (но не повече от по 3) отговарят на различни изисквания. Най-слабо е нивото на изпълнение по отношение на изискванията за наличие на вътрешни правила и инструкции за управление на достъпите, за наличието на вътрешни правила за проверка на актуализациите преди инсталирането им, за наличие на вътрешни правила и инструкции за действие за прилагане на актуализациите.

2) Изисквания за конфигуриране

- Предвидените в Прил. №4 на НМИМС, изисквания за конфигуриране се изпълняват непълно от трите категории общини.

- Една община първа категория, изпълнява 11 изисквания (от общо 12), 1 община - 10 изисквания, 1 община - 9 изисквания, 1 община - 7 изисквания и 1 община - 4. Нито една община не изпълнява изискването за забрана на настройка „Everyone“, при споделено ползване на

файлове и принтери. Всички общини са конфигурирали „User Account Control“ на най-високо ниво така, че винаги да се дават необходимите предупреждения.

- Забрана на „Pop up“ браузерите и конфигуриране на „Auto play“ функцията винаги да иска потвърждение от потребителя са приложени от всички общини втора категория. Най-малък е броят (2) на общините забранили „Auto Complete“ и „Trace Track“ метода.

- Едно от изискванията е приложено от всички общини трета категория. Най-нисък е броят (2) на общините приложили изискванията относно забраната на „TLS renegotiation“ в системи, използващи TLS, или да се конфигурира „rate-limiter“ за ограничаване на броя на предоговаряне на сесия и за необходимостта да се използват приложения (add-ons) към браузърите за блокиране на рекламно съдържание.

ИЗВОДИ:

- В значителна степен се различават по тип изискванията, които са приложили трите категории общини. Причините за неприлагане на всички изисквания се крият в някои специфични особености при ограничен брой от изследваните общини, както и недостатъчна експертиза на служителите, които следва да ги реализират.

- Защитата от уязвимости днес се счита за един от основните проблеми на МИС. Почти всеки ден се откриват нови уязвимости в използвания софтуер, включително и за такъв, използван от общините. Независимо от факта, че доставчиците на хардуер и софтуер непрекъснато се усъвършенстват и предоставят подходящи корекции, такива корекции водят в повечето случаи до необходимостта от обработка на значително количество информация и значителни работното натоварване, свързано с тяхното приложение.

- Има значителната разлика в ефективността между единични (напр. годишни) оценки на уязвимостта и текущ процес на идентифициране и коригиране на уязвимости. Ако корекциите не се правят редовно, ИКС остават уязвими за злонамерени средства твърде дълго и рискът от успешна кибератака нараства значително. Информацията, получена от изследваните общини по този въпрос не позволява достатъчно увереност, че този проблем се решава по адекватен и последователен начин.

ПРЕПОРЪКИ:

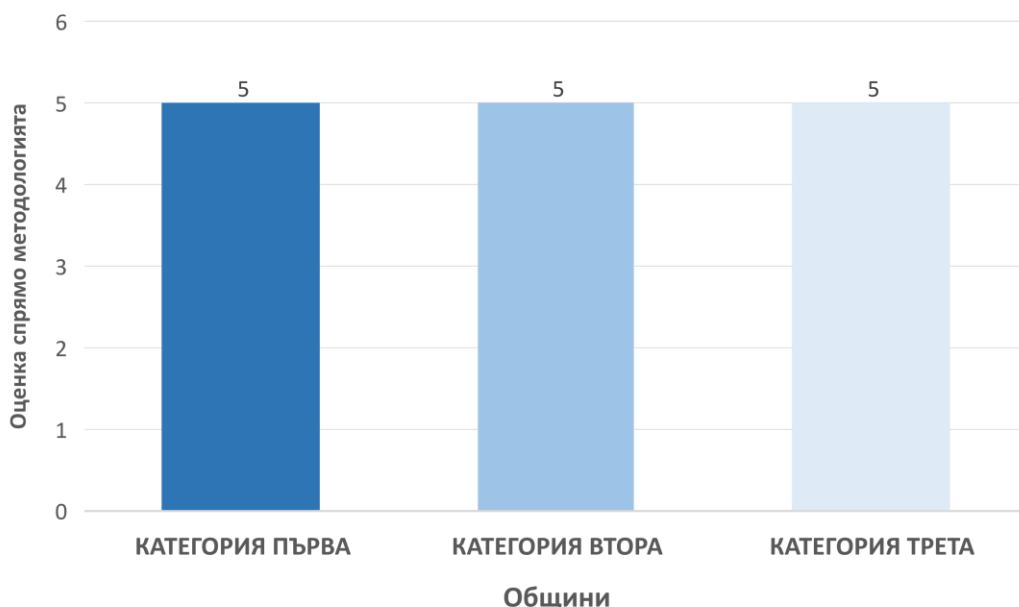
- Екипът препоръчва на Ръководителите на общини неизпълнили изискванията по чл.22 и Прил.4, от НМИМИС да планират необходимите действия за изпълнението им. Дейностите следва да бъдат изпълнени от служители(или доставчици на услуги) притежаващи необходимата експертиза за това.

- За актуална информация относно новооткрити уязвимости и начини за неутаризирането им препоръчваме да се използва сайта на Националния екип за реагиране при инциденти с компютърната сигурност govcert.bg.

23. Защита от зловреден софтуер

Резултати:

■ ЗАЩИТА ОТ ЗЛОВРЕДЕН СОФТУЕР



Фигура 22 резултати от проведено проучване по т. Защита от зловреден софтуер.

КОНСТАТАЦИИ:

- Две от общините първа категория са приложили всичките 6 изисквания; Най- малък са общините (3 бр.) изпълнили изискването за извършване на периодична оценка на ефективността на мерките за защита от зловреден софтуер.
- Всички общини втора категория прилагат всички изисквания за защита от зловреден софтуер.
- Четири общини трета категория прилагат всички изисквания. В тази категория общини, най-слабо се прилагат мерки за изпълнение на изискването за извършване на периодична оценка на ефективността на мерките за защита от зловреден софтуер.

ИЗВОДИ:

- Изискванията по чл.23 „Защита от зловреден софтуер“ са едни от тези, които се прилагат в практиката на почти всички общини в голяма степен.

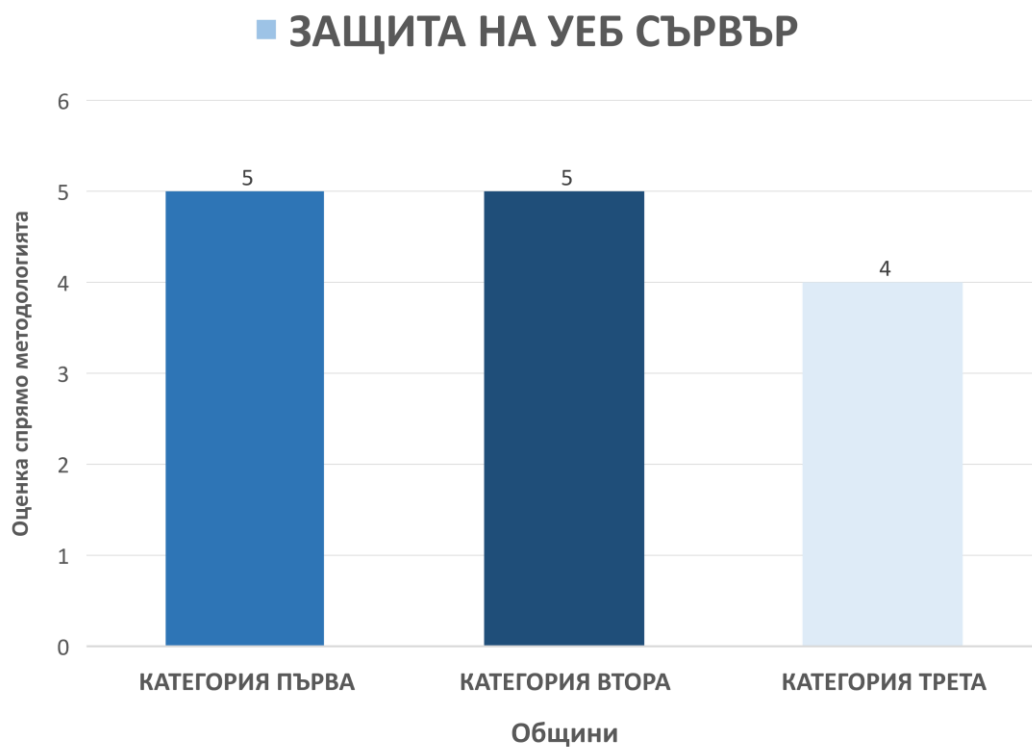
ПРЕПОРЪКИ:

- Екипът препоръчва на Ръководствата на всички общини да продължат да прилагат изискванията за защита от зловреден софтуер, като онези общини, които минимални пропуски следва да ги отстранят

24. Защита на уеб сървър

Резултати

23:

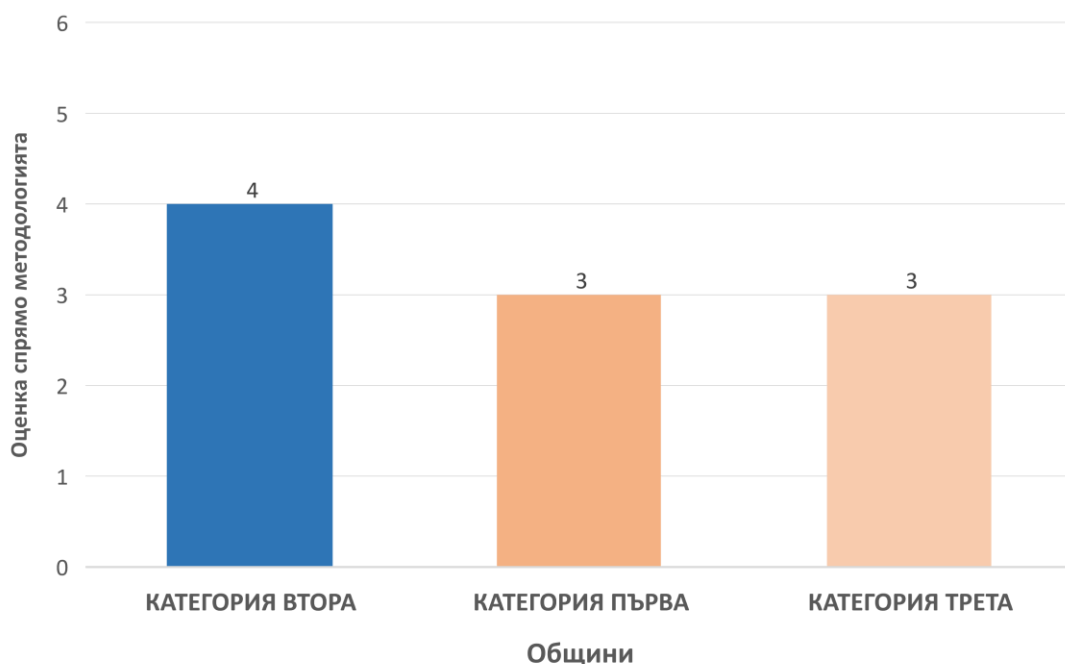


Фигура 23 Резултати от проведено проучване по т. Защита на уеб сървър.

25. Изисквания към headers на отговорите на заявки за уеб сайтове

Резултати:

ИЗИСКВАНИЯ КЪМ HEADERS НА ОТГОВОРИТЕ НА ЗАЯВКИ ЗА УЕБ САЙТОВЕ



Фигура 24 Резултати от проведено проучване по т. Изисквания към headers на отговорите на заявки за уеб сайтове.

КОНСТАТАЦИИ:

1) Защита на уеб сървъри

- Три общини първа категория са изпълнили всички 20 изисквания по чл.24. „Защита на уеб сървъри“, 2 общини са изпълнени 12 изисквания.

- Сравнително висок е и броя -7, на изискванията приложени от всички общини втора категория. Ниска е степента на прилагане по изискванията да има сложен файл „robots text“ и при използване на Система за управление на съдържанието (CMS) да се промени наименованието по подразбиране на папката за достъп до администраторския панел – където само 1 и съответно 2 общини са ги приложили.

- При общините трета категория, степента на прилагане на изискванията по чл.24 е значително по-ниска. Там няма нито едно изискване, което да е изпълнено едновременно (заедно) от всички общини 8 изисквания са изпълнени от по две общини, а изискването „всички данни, изпращани от клиента и показвани в уеб страница, да бъдат кодирани с HTML, за да се гарантира, че съдържанието се изобразява като текст вместо HTML елемент или JavaScript“ е изпълнено от само една община.

2) Изисквания към headers на отговорите на заявки за уеб сайтове.

- Приемливо е нивото на изпълнение на изискванията по Прил. №5 от Наредбата, за общините първа категория. На 5 от изискванията отговарят 3 общини, на другите две изисквания – 3 общини.

- На всичките 8 изисквания отговарят три общини от втора категория.

- Удовлетворително е нивото на изпълнение на изискванията по Прил. №5 от НМИМИС за общините трета категория. При тази категория всяко едно от изисквания е изпълнени от само по две общини.

ИЗВОДИ:

- Степента на прилагане на изискванията за защита на уеб сървъри в различните категории общини е различна. Общините първа и втора категория прилагат по-голямата част от изискванията, докато при общините трета категория има дефицит от прилагането на тези изисквания. Предвид важността и мястото на уеб сървърите в архитектурата на мрежите в общините може да се направи обосновано предположение, че степента на МИС на уеб сървъри в третата категория общини е недостатъчна. Недооценяване значението на спазване на тези изисквания от някои общини е възможна предпоставка за киберинциденти, включително и на такива с по-висок приоритет.

- По отношение на изискванията на Прил. №5 от НМИМИС „Изисквания към headers на отговорите на заявки за уеб сайтове.“ е налице известно подценяване от общините първа и най-вече трета категория.

- За общините, при които Headers на отговорите на заявките съдържат информация за платформите и версиите на използвания софтуер, то това би улеснило злонамерено използване на тази информация за възможни кибератаки. Ако Headers, не поддържат опцията X-XSS-Protection, няма да може да се настройва конфигурацията за XSS филтъра, вграден в повечето браузъри. Когато филтъра може да се настройва създава условия за предотвратяване на някои категории XSS атаки;

ПРЕПОРЪКИ:

- По отношение защитата на уеб сървъри, Екипът препоръчва на ръководствата на общини първа и втора категория, да продължат практиката за прилагане на изискванията, с тенденция установените пропуски да бъдат отстранени.

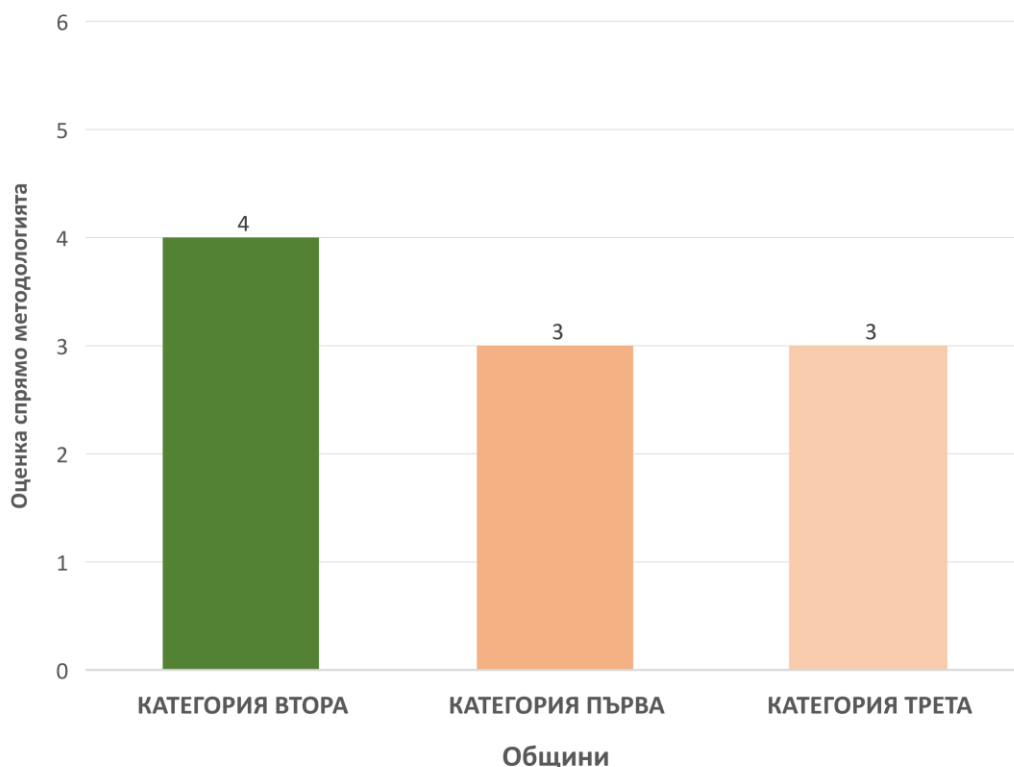
- На ръководствата на общини трета категория, които не прилагат изискванията, екипът препоръчва да предприемат необходимите адекватни мерки за защита сървърите, като по този начин ще намалят вероятността за успешни кибератаки срещу тях.

- По отношение на изисквания към headers на отговорите на заявки за уеб сайтове и предвид установената степен на прилагане, екипът смята, че тук е необходимо ръководителите на общини и от трите категории, които не изпълняват тези изисквания да възложат на лицата (собствен персонал или външен доставчик на такава услуга), които поддържат уеб сайта на общината да предприемат необходимите дейности за изпълнение на изискването.

- Като възможна мярка екипът, препоръчва да се установят контакти с Министерство на електронното управление с цел: използване ресурса на Държавния хибриден частен облак в интерес на общините; хостване на общински сайтове от МЕУ.

26. Защита на DNS

■ ЗАЩИТА НА DNS



Фигура 25 Резултати от проведено проучване по т. Защита на DNS.

Констатации:

- Само две общини първа категория прилагат 4 (от общо 6) от изискванията за защита на DNS и едно изискване се прилага от три общини, а едно да се забрани „zone-transfers“ от една община.

- При общините втора категория, за всички изисквания се прилагат мерки от само две общини, а една община изпълнява 5 от тези изисквания.

- Три общини трета категория изпълняват всички изисквания. Неспазването в такава степен на изискванията на чл.25. „Защита на DNS“, от НМИМИС е предпоставка за увеличаване на броя успешни кибератаки срещу общините неизпълнили това изискване. Така например ако не се забрани zone-transfers, то злонамерени лица могат бързо да определят всички хостове в определена зона чрез трансфери на DNS зони, да събират информация за домейна, да избират цели за атаки, да откриват неизползвани IP адреси и да заобикалят мрежовия контрол на достъпа, за да крадат информация.

ИЗВОДИ:

- Спазването на изискването за прилагане на мерки за защита на DNS, е подценено в известна степен.

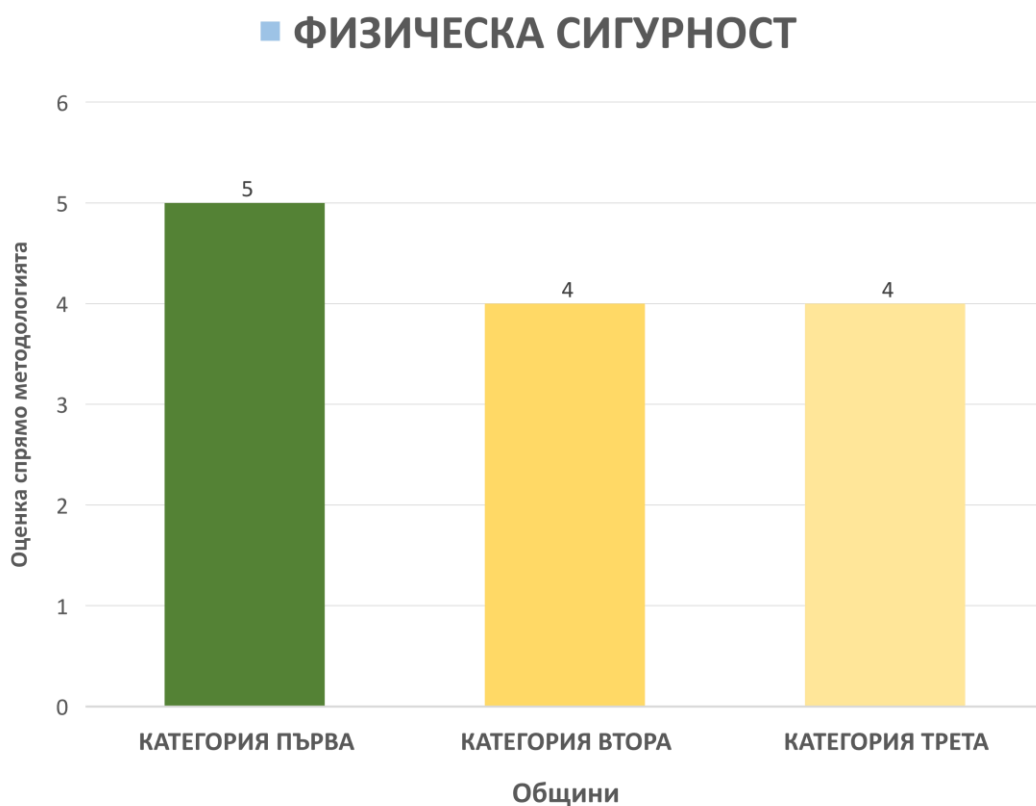
- Съществува реална опасност от повишено ниво на заплахи от успешни и различни видове кибератаки към общините неизпълнили тези изисквания.

ПРЕПОРЪКИ:

- Екипът препоръчва на ръководителите на общини неспазващи изискванията за защита на DNS, да вземат мерки за осигуряване защита на тези сървъри.

- Като възможна мярка екипът, препоръчва да се установят контакти с Министерство на електронното управление с цел използване ресурса на Държавния хибриден частен облак в интерес на общините.

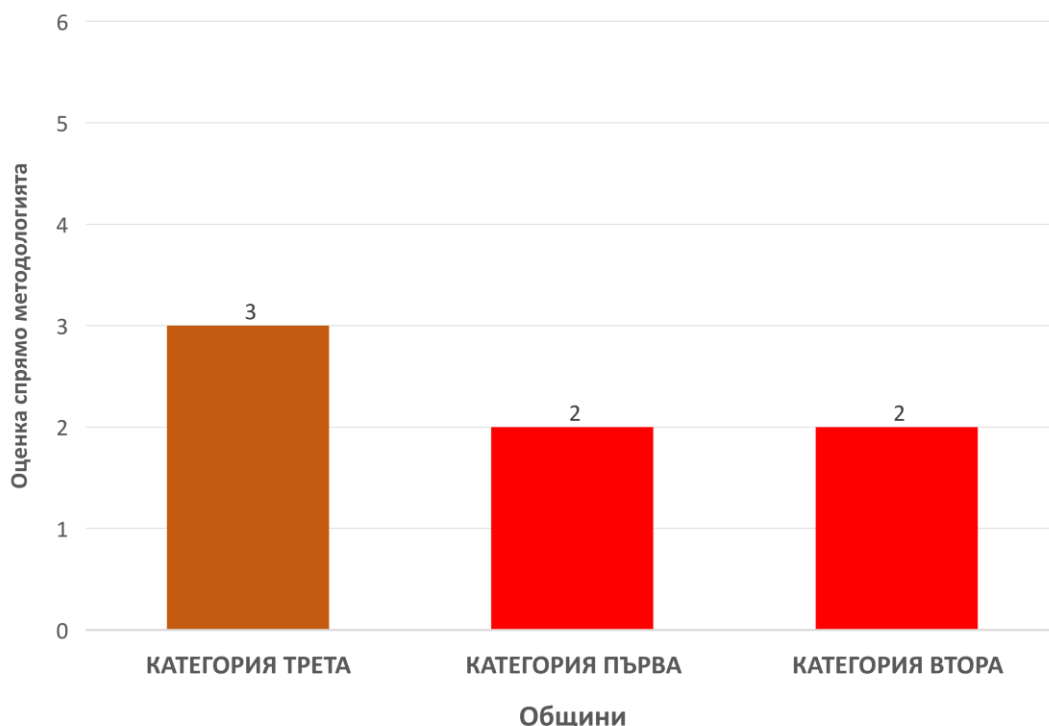
27. **Физическа сигурност.**
Резултати:



Фигура 26 Резултати от проведено протличенчване по т. Физическа сигурност.

28. **Наблюдение***
Резултати:

■ НАБЛЮДЕНИЕ



Фигура 27 Резултати от проведено проучване по т. Наблюдение*

КОНСТАТАЦИИ:

1) Физическа сигурност

- Почти всички общини първа и втора категория са взели необходимите мерки за обезпечаване на физическата сигурност на информационните активи.

- Общините трета категория са осигурили в голяма степен защитата на информационните активи, а наблюдението им се извършва от 4 общини (от всичко 6)

- Независимо, че текста по-долу не е пряко следствие от изследването, Екипът смята, че не е излишно да сподели някои свои виждания по въпроса за релация между физическа сигурност и МИС.

- Донякъде философският въпрос дали МИС се разглежда предимно като „кибер“ проблем с информационните технологии или сигурността (сравним с физическия защита и сигурност), но пренесени в дигиталната сфера стои на дневен ред отдавна, още на етапа на концептуализация на този проблемен въпрос. На практика физическата сигурност и МИС имат редица общи черти. В момента системи, които осигуряват функции за сигурност и защита, които не използват никаква форма на ИКТ са по-скоро изключение, отколкото правило. В резултат на това последствията от нарушения на МИС и засягането на такива системи може да се материализира във физическия свят, понякога дотолкова, че засяга живота или физическата почтеност на хората.

- Не липсват примери за това как МИС и физическата сигурност се пресичат на практика. Например, хакерите могат използвайки слабостите в протоколите за сигурност да внедрят шпионски софтуер на електронни устройства или да качат поверителна информация на преносими устройства, да получат онлайн достъп до планове за офис пространство за избор на за кражба на лични данни. В допълнение, ненадеждни мерки за сигурност, застрашаващи защитата на помещения, центрове за данни, сървърни помещения или ключови цифрови точки

от неоторизиран достъп или други форми на неоторизирана намеса, произтичаща от физически опасности, могат да имат преки неблагоприятни ефекти, в дигиталната сфера.

- В преобладаващата част от изследваните общини институционалните връзки между физическа сигурност и МИС са по-скоро спорадични. При провеждане на интервюта с длъжностни лица се установиха различия в степента на осъзнаване на връзката между физическата сфера и МИС.

2) Наблюдение

- Само една община първа категория и две общини трета категория имат изградени системи за автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността ИКС, чрез анализ на информационни потоци, протоколи и файлове, преминаващи през ключови устройства, позиционирани така, че да могат да анализират всички потоци, обменяни между собствените им ИКС, както и с ИКС на трети страни. От общините втора категория нито една няма изградена такава система.

ИЗВОДИ:

- Обезпечаването на физическата сигурност на информационните активи стои на вниманието на Ръководителите на общини. В по-ниска степен е изпълнена мярката за обезпечаване на изискването за наблюдението на информационните активи.

- В тринадесет общини (от общо 16) е подценена необходимостта от изграждане на гореспоменатата система за откриване на събития в резултат, на което готовността на тези общини за своевременно откриване и неутрализиране на заплахи за МИС е минимизирана.

ПРЕПОРЪКИ:

- Ръководителите на общини да продължат поддържането на високо ниво на обезпечаване на физическата сигурност, като насочат усилията си за подобряване наблюдението на информационните активи.

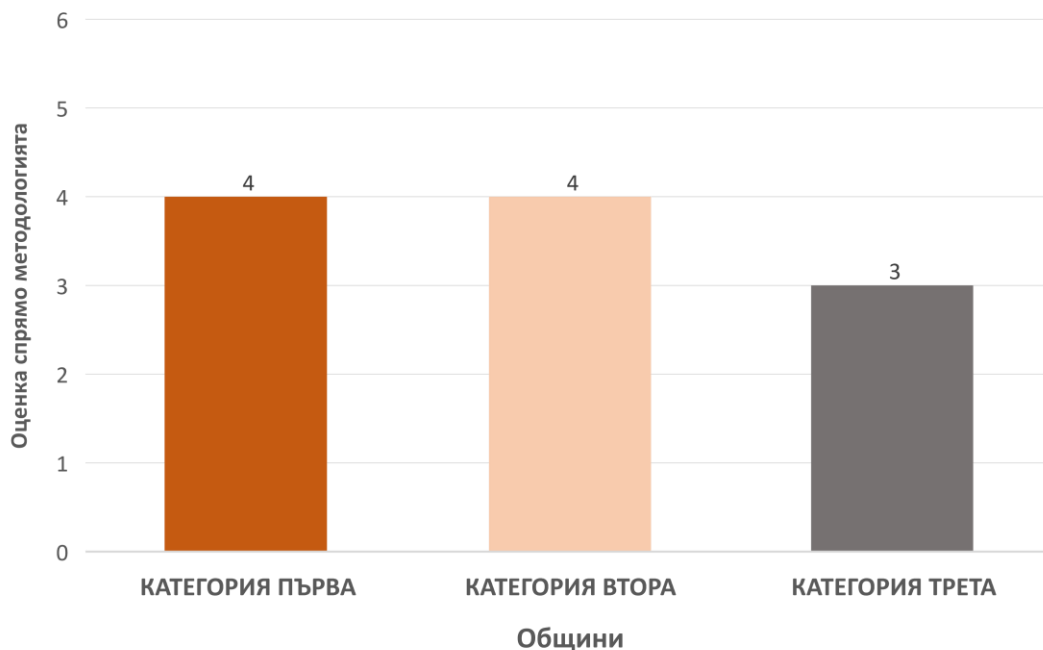
- Ръководителите на 13-те общини, които нямат система за откриване на събития да предвидят в бюджетните си прогнози за следващата година финансови средства за изграждане на такива системи.

- Доизграждане на собствена система за наблюдение, екипът препоръчва на ръководителите на тези общини, да използват възможностите на доставчици на услуги по наблюдение в рамките на техен Оперативен център за сигурност (SOC- Security Operational Center).

29. Системни записи

Резултати:

■ СИСТЕМНИ ЗАПИСИ



Фигура 28 Резултати от проведено проучване по т. Системни записи.

КОНСТАТАЦИИ:

- Три общини от първа категория изпълняват всички изисквания по чл.19. „Системни записи“. Най-слабо е изпълнено изискването за наличието на сървъри за приложения, които следва да поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, просмени в правилата за сигурност и функциониране на информационните и комуникационните системи.

- От общините втора категория също 3 са изпълнили всички изисквания. Най- слабо е изпълнено изискването информацията за системните записи да се съхранява най-малко една година.

- Две общини трета категория изпълняват всички изисквания по чл.29. Най-слабо са изпълнени изискванията за синхронизация на часовниците на компоненти на ИКС, за необходимостта за използване на протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен и за Регламентиране на достъпа до системните записи само до лица, имащи задължения за наблюдението по смисъла на чл. 30, за разрешаването на инциденти с мрежовата и информационната сигурност, за разкриването и разследването на тежки престъпления и престъпления по чл. 319а–319е от Наказателния кодекс в съответствие с чл. 14, ал. 4, т. 2 и чл. 15, ал. 3, т. 3 от Закона за киберсигурност.

ИЗВОДИ

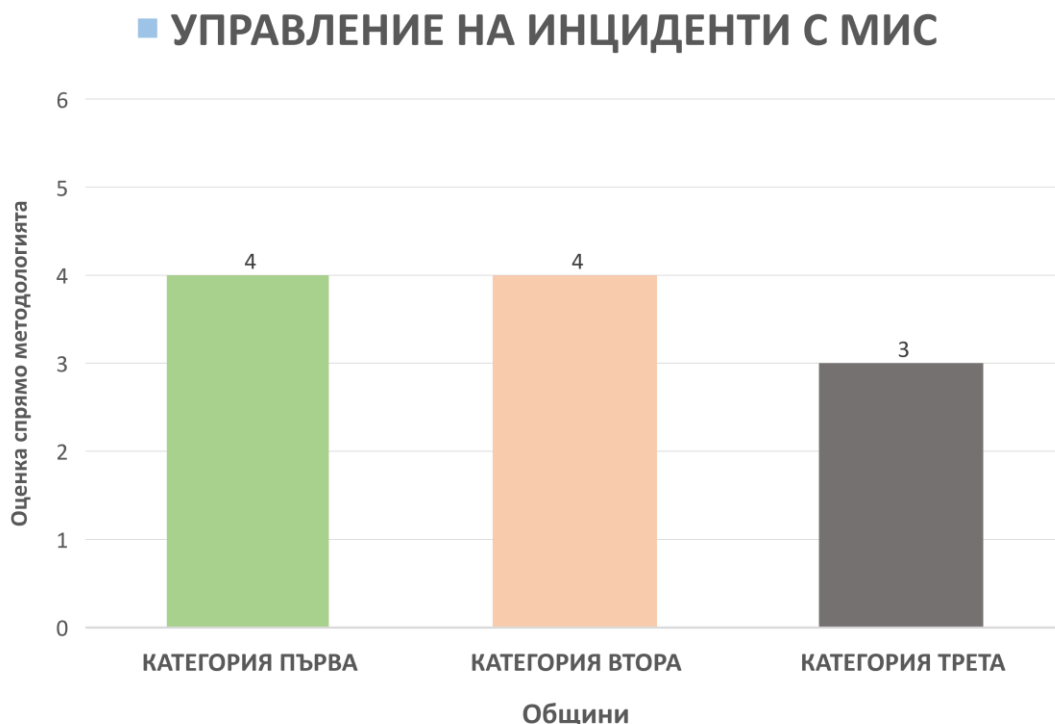
- Броя на общините изпълнили изискванията по чл.19, е твърде малък. Подценено е значението на информацията от системните логове за предприемане на проактивни и реактивни дейности ИКС.

ПРЕПОРЪКИ:

- Да се прецени важноста от използването на информация от системните записи и Ръководителите на общини където не са изпълнени изисквания да организират изпълнението им.

30. Управление на инциденти с МИС

Резултати:



Фигура 29 Резултати от проведено проучване по т. Управление на инциденти с МИС

КОНСТАТАЦИИ:

- В три общини първа категория са разработени и се прилагат мерки в съответствие с всички 11 изисквания по чл.32 от НМИМИС. Две общини не са изпълнили нито едно от изискванията за управление на инциденти с МИС.

- Четири общини от втора категория са декларирали, че изпълняват всички изисквания за управление на инциденти, а една община не е изпълнила нито едно изискване.

- Три общини трета категория отговарят на 5 (от общо 6) изисквания, 3 общини не изпълняват 4 от изискванията. По този повод екипът смята, че в тези общини и по това изискване е налице недобро управление на инциденти в МИС.

- Според съществуващи добри практики, за тестване на канали за достъп до ръководни органи, следва на тези органи да се доведе до знанието следната ключова информация.

а) тежестта на инцидента;

б) очаквано въздействие върху дейностите на общината;

в) въздействие върху процеси свързани с взаимодействие с трети страни;

г) вероятността инцидентът да стане публично известен.

- Екипът обръща внимание и на факта, за необходимост за докладване за регистриран инцидент с МИС в общините, до Националния екип за реагиране при инциденти с компютърната сигурност (който изпълнява функциите и не секторен екип за публичната администрация).

- По време на инцидентът на вниманието на органа за вземане на решения следва да се предложат предпазни мерки за предотвратяване и неутрализиране на конкретни уязвимости както и информация за способността на общината да предприеме тези мерки за реагиране.

Инцидента трябва да бъде доведен своевременно до вниманието на органа, вземащ решения, преди да се случи пълно увреждане, или по-скоро, веднага щом станедостатъчно ясно, че се случва. Такова уведомяване веднага след откриване на атака от друга страна не бива да е твърде рано извършено, защото по този начин може да се наруши установения алгоритъм на усилията за разрешаване на инцидента. В същото време, ако се забави информирането на органа за вземане на решения до пълното разрешаване на инцидента, тогава това може да постави под въпрос доверието на ръководството на общината.

- След прецизно извършване на анализ и оценка на риска е напълно възможно да се окаже, че е налице хибриден подход. При него както вече беше споменато по-горе в анализа собствен ИТ и МИС персонал, в допълнение с доставчици услуги (трети страни) по МИС, формират подходящо решение за по-висока устойчивост на система за МИС.

- Трябва да съществуват планове за дейностите в случай на кибератаки и на инциденти. За своевременно взимане на решения от оправомощените органи е важно в общините да има ясен механизъм, чрез който на ръководството на общини да им бъде предоставена необходимата им информация за кибератаки. Тъй като вероятността от подобни атаки може да се предвиди то следва, че подробен план за разрешаване на кибер инциденти трябва да е разработен предварително.

- Вземане на решения, което предполага импровизация по време на остра криза, е вероятно да бъде затруднено от необходимостта от ситуационни антикризисни мерки, докато спазването на установения план би дало пълна възможност за изостряне внимание на специфични параметри, които неизбежно присъстват във всеки конкретен случай. В допълнение, необходимостта от разработване на такива мерки в условията на криза ще направи процеса по-малко уязвим за неправомерно влияние. И на края, би било уместно да се вземат предвид възможностите на ръководството да обсъди собствения си алгоритъм на действие при възникване на кибератаки когато бъдат уведомени за тях и те следва да вземат решения. Този подход може да помогне за установяване някои внимателно обмислени и договорени граници на действие, предприети от ръководството, които от своя страна насърчават информираното вземане на решения в тази потенциално чувствителна зона.

- Налице е ограничена готовност за предоставяне данни на националните органи (Националния екип за реагиране при инциденти с компютърната сигурност - НЕРИКС), изследваните общини не са докладвали нарушения на МИС на НЕРИКС.

ИЗВОДИ:

- Малък е общия брой общини приложили всички изисквания за управление на инциденти с МИС.

ПРЕПОРЪКИ:

- Екипът препоръчва на ръководствата на общините изпълнили цялостно изисквания по чл.30 и чл.31 от НМИМИС да предприемат необходимите организационни мерки за цялостно изпълнение.

- Екипът препоръчва да се прилага многостранен подход за управлението на инциденти, който да обхваща всички нива на общините - от органи на управление; органите за надзор, административно управление; ръководители на структурни звена и единици; както и служителите като цяло.

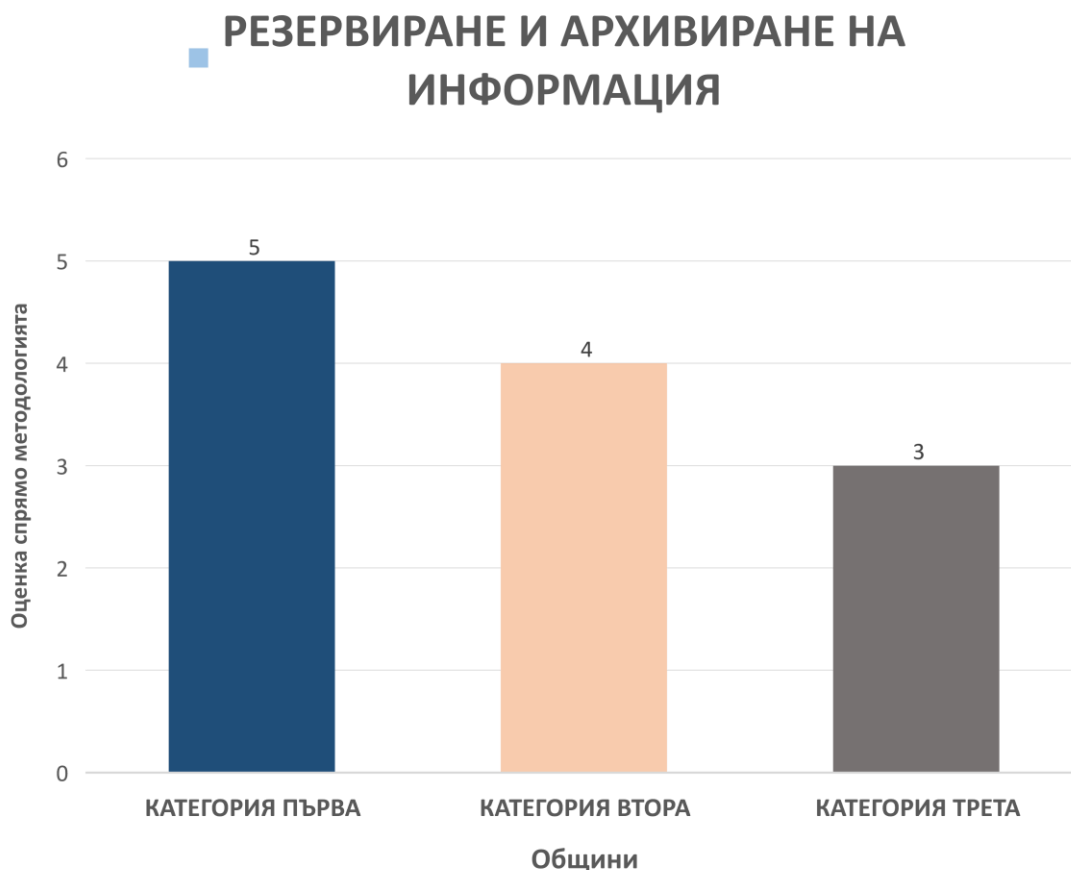
- Освен това функционалността на тази област изисква по-широк поглед, който надхвърля рамка на ИКТ и директно вписване на МИС в практиката за управление на риска в общината.

- Препоръчва се да бъде насърчавано желание за прозрачност и поемане на отговорност за възможни пропуски в системата за МИС. Следва да стане практика, разбирането на общините, че служители и звена които открито съобщават на своите органи за вземане на решения и управление за инциденти за недостатъци в тяхната киберзащита не трябва да се страхуват, тъй като загубата на репутация, включително загубата на доверие от ръководствата

далеч надхвърлят възможните последици от щети, включително непреки финансови последици, в резултат на атаката.

РАЗДЕЛ III – УСТОЙЧИВОСТ

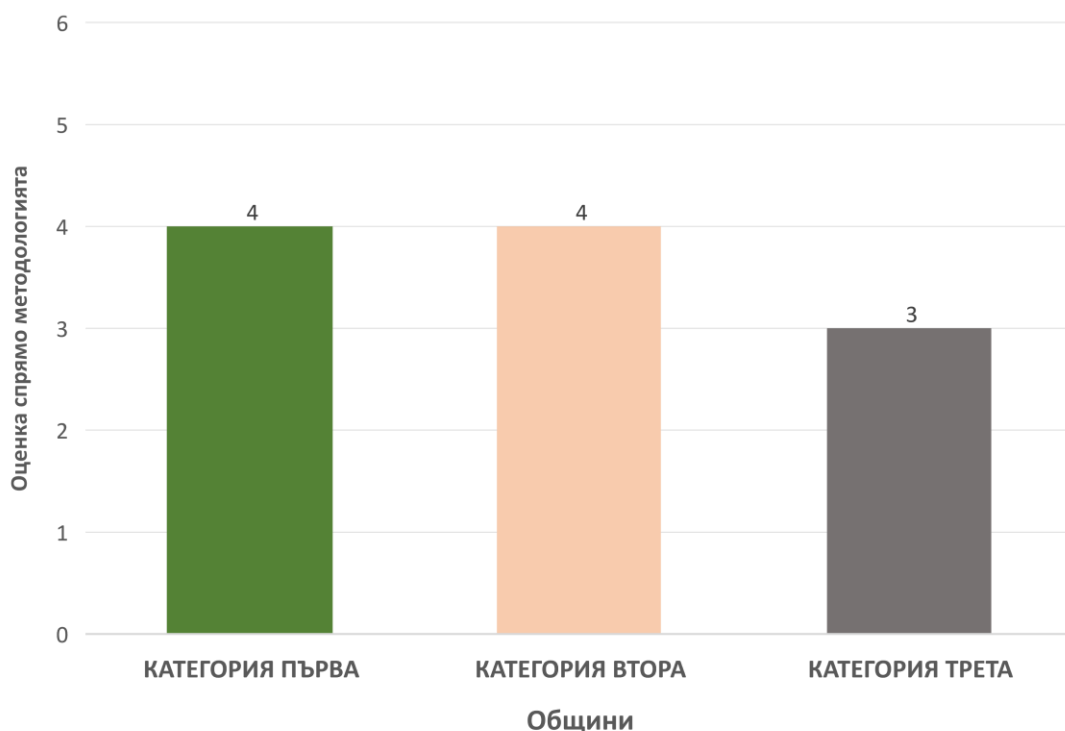
31. Резервиране и архивиране на
Резултат 30:



Фигура 30 Резултати от проведено проучване по т. резервиране и архивиране на информация.

32. Резервиране компоненти на инфраструктурата*
Резултати:

РЕЗЕРВИРАНЕ КОМПОНЕНТИ НА ИНФРАСТРУКТУРАТА



Фигура 31 Резултати от проведено проучване по т. Резервиране компоненти на инфраструктурата*

КОНСТАТАЦИИ:

1) Резервиране и архивиране на информация

- Всички общини от първа категория са покрили 12 (от общо 15) изисквания отнасящи се до чл. 32. „Резервиране и архивиране на информацията“ от НМИМИС. Две общини не са покрили останалите три изисквания относно необходимостта във Вътрешните правила да резервиране и архивиране, да се посочва точното място за съхранение на всяко копие, случайте за използването на всяко копие и за извършване на проверка за годността на копията за използване през 2022 г.

- Шест изисквания са изпълнени от по 4 общини втора категория, а останалите 9 изисквания от по 3 общини.

- От общините от трета категория, 3 са изпълнили, 5 изисквания, съответно 4 са изпълнили по 7 от изискванията, а две общини са изпълнили по 1 изискване. Най-слабо изпълненото изискване се отнася до наличието на планове за действия в случаи на авария, природни бедствия или други непредвидени обстоятелства.

2) Резервиране на компоненти на инфраструктурата

- Една община от първа категория не е резервирала компоненти на инфраструктурата.

- Две общини втора категория не са резервирали компоненти, а от трета категория този брой общини е 4.

ИЗВОДИ:

- Част от общините най-вече първа, отчасти втора и в по-малка степен трета категория са създали мерки за изпълнение на изискванията както по отношение резервирането и

архивирането на информация, така и по отношение резервирането на компоненти от инфраструктурата.

- Има обаче и общини които не създавайки условия за резервиране и архивиране на информация съгласно изискванията рискуват при инцидент с МИС да им бъде открадната и да загубят цялата си налична информация или част от нея.

- Липсата на резервираност на основни компоненти ил системи в някои общини понижава значително тяхната киберустойчивост и възможностите им за бързо и гъвкаво възстановяване в случай на инцидент.

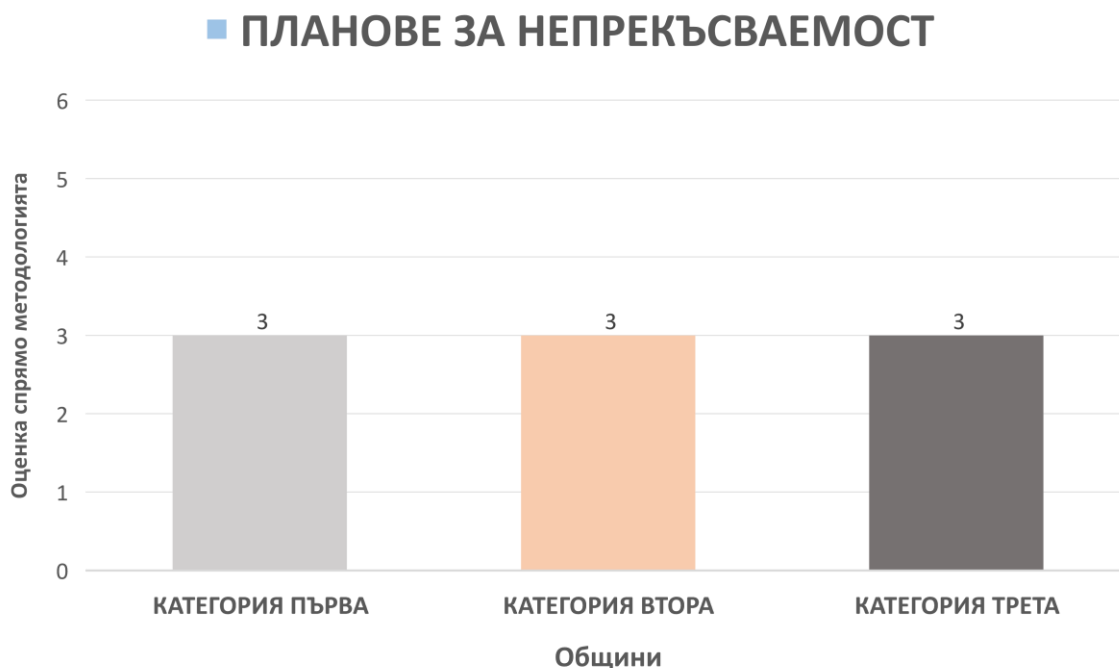
ПРЕПОРЪКИ:

- Ръководителите на неизпълнилилите изисквания общини, да предприемат мерки включително и да създадат условия за резервиране на информация и за жизненоважните компоненти от инфраструктурата им.

- Като възможна мярка екипът, препоръчва да се установят контакти с Министерство на електронното управление с цел използване ресурса на Държавния хибриден частен облак в интерес на общините.

33. *Планове за непрекъсваемост*

Резултат:



Фигура 32 Резултати от проведено проучване по т. Планове за непрекъсваемост.

КОНСТАТАЦИИ:

- Екипът констатира ниско ниво на изпълнение на това (заедно с изискване 27. „Наблюдение“) от изследваните общини спрямо всички останали изисквания на Наредбата.

- Три (от общо 6) изисквания са изпълнени от 2 общини първа категория, 1 община е изпълнила три изисквания и 2 община са изпълнили едно изискване. В категорията няма нито една община, която да е изпълнила всички изисквания.

- Общините втора категория е установено, че три от тях изпълняват 3 от изискванията, 1 община отговаря на едно изискване и две общини – на две изисквания.

- Резултатите за общините трета категория са аналогични на тези от втора категория.

ИЗВОДИ:

- Преобладаващ брой общини са пренебрегнали изпълнението на това изискване. Това от своя страна е предпоставка в случай на прекъсване нормалната работа на ИКС на общините да се създаде смут, деорганизация, взимане на неадекватни и панически решения.

- В общините, би било удачно да се прилага концепция за планиране на устойчивостта, в която един от многото аспекти е МИС. Основната задача на тази област на организационна устойчивост е да се оценят адекватно рисковете за МИС, за да се предприемат превантивни мерки, мерки за намаляване на риска и защита от заплахи от една страна и внедряването на адекватни протоколи за управление и действия, за поддържане на непрекъснатост на дейностите на общината в случай на реализиране на такива рискове.

- Намаляването на рисковете за МИС разбира се не е абсолютно, а по-скоро е въпрос на степен и на нейната ефективност, т.е. трябва да се оценява не само по успеха в предотвратяването на заплахи, но и по отношение на степента, в която може да помогне за възстановяване на нарушената дейност в резултат на кибератаката. Ето защо, в случай на сериозен инцидент, е важно в общината да има добре установена процедура за възстановяване след възникване на проблеми във всяка една от наличните ИКС. Това може да се постигне само ако протоколите и дейностите по възстановяване са обхванати в нарочен план за непрекъсваемост. Освен това те следва редовно и щателно да се тествани като част от нормалното планиране на непрекъснатостта на дейностите в общината.

- Плановите за непрекъсваемост след инцидент и процедурите за възстановяване съдържащи се в него, са силно технически компонент. За да бъдат ефективни, те трябва да се развиват в рамките на стратегическите параметри, определени от ръководството на общината (включително граници на приемлив риск, налични ресурси и т.н.), и налични оперативни ограничения (като приемливи за възстановяване информационни активи). Съответно планирането на непрекъснатостта на дейностите в общината, заедно с контрола на риска, следва да е неразделна част от планиране устойчивостта на дейността както за физически заплахи, така и за кибер заплахи.

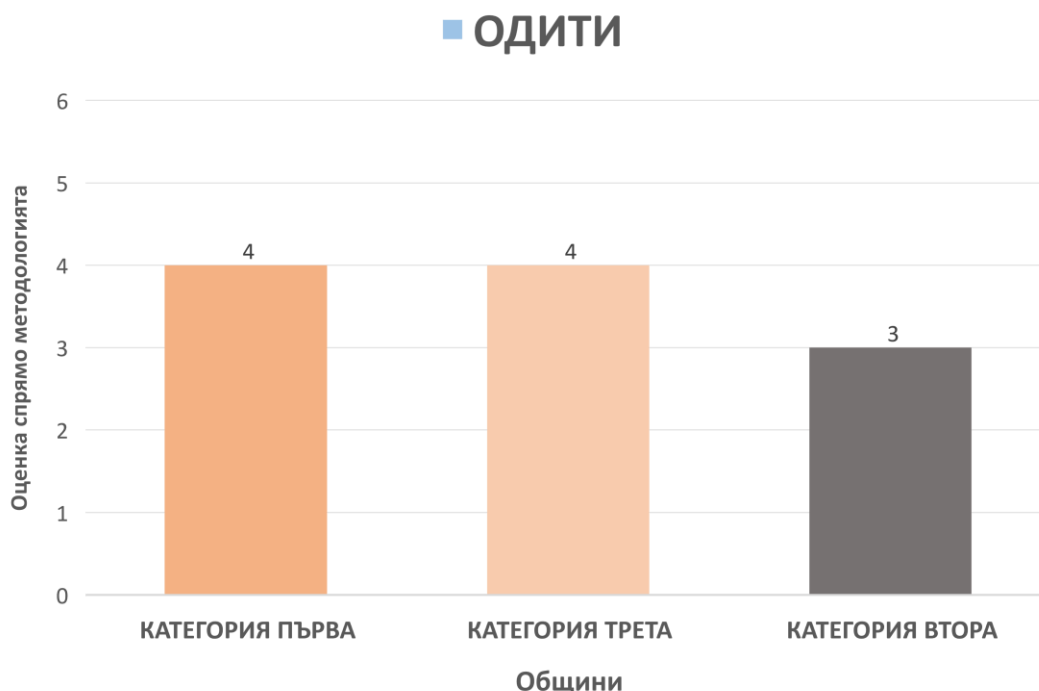
ПРЕПОРЪКИ:

- Предвид гореизложеното, екипът препоръчва ръководствата на общини, които нямат или не поддържат в актуално състояние, Планове за непрекъсваемост, да вземат мерки в обозрими срокове да се изпълнят изискванията. За изпълнението на тази препоръка не са необходими финансови ресурси.

ГЛАВА ТРЕТА – КОНТРОЛ

34. .Одити

Резултати:



Фигура 33 Резултати от проведено проучване по т. Одити.

КОНСТАТАЦИИ:

- Екипът в процеса на изследване и последвалите го интервюта и фокус групи проучи практиката за решаване на проблеми от надзорните органи в МИС в контекста на съответните им области на дейност, независимо дали са на ниво на функцията за вътрешен одит (насочена основно към оценка спазване на правила и процедури), на ниво външен одит (основно свързан с проверки за съответствие, а понякога и с проверки за ефективност в административни и управленски области).

- Едно от направленията на одитите е насочено основно към ИКС, и в най-голяма степен към МИС. Въпросите, свързани с ИКС, обикновено се вписват добре в базираното на риска планиране на вътрешния одит. В рамките на поведените фокус групи и интервюта, екипът не установи общини, които имат специализирани надзорни органи за извършване на одит по смисъла на чл.35, ал., т. 1 от НМИМИС. В общините, които извършват вътрешни одити, тези функции по правило се изпълняват от щатните звена за вътрешен одит. Независимо, че по принцип на тези звена липсва компетентност в сферата на МИС, то по отношение одитиране нза наличие на документи и процедури, тяхната дейност е полезна, макар и непълна.

- В повечето случаи този подход изглежда задоволителен. Втория тип общини имат област на фокус за външни одитори, такива, които се занимават с теми като например, оценка на риска и управление на риска, правила в областта ИКТ и управление препоръки и предложените стъпки за изпълнението им.

- Четири от общините първа категория са декларирали, че през 2022г., при тях е извършен външен одит по смисъла на чл. 35, ал. 1, т. 1 и т. 3, от НМИМИС.

- Две от общините втора категория са извършили външни одити, а от трета категория - три общини са направили одит.

ИЗВОДИ:

- При одитите наред с други неща са идентифицирани рискове за МИС, като някои от тях са свързани с процесите на дигитализация. При одитите основно внимание е отделено на управлението на риска или, когато е приложимо, и когато е проследимо от предходни одити, състоянието на изпълнение на препоръките от вътрешен или външен одит, свързан с ИКТ.

- Цел на резултатите от тези одити е и подпомагане на ръководството при прилагането на подход към МИС, базиран на оценка на риска, не за информирането им относно съответните рискове за МИС.

ПРЕПОЪКИ:

- Стойността на препоръките на одитните органи за подобряване на състоянието на МИС в общините да намира израз, като минимум насърчава положителните промени, (например подчертаване на необходимостта от специалисти по МИС) систематично да осигурява наличие на максимална възвращаемост от дейността на одитни (надзорни) органи в областта на МИС.

В опит да се даде обща представа за текущото състояние анализът показва как участващите общини оценяват цялостната си система за МИС в широки категории дефинирани функционални области в специално създадения за целите на анализа, въпросник.

В резултат от получените отговори по въпросника и съгласно Методологията за изследване и мониторинг на ефективното прилагане на НМИМИС от общините 1, 2 и 3 категории, участващи в Проект - BG05SFOP001-2.025 „Повишаване на общото ниво на мрежова и информационна сигурност в общински администрации“ са получени следните оценки:

<u>ОБЩА ОЦЕНКА:</u>
ЗА ОБЩИНИТЕ ПЪРВА КАТЕГОРИЯ, Е: ДОБЪР – 4.09
ЗА ОБЩИНИТЕ ВТОРА КАТЕГОРИЯ, Е: ДОБЪР – 4.06
ЗА ОБЩИНИТЕ ТРЕТА КАТЕГОРИЯ, Е: УДОВЛЕТВОРИТЕЛЕН – 3.46

Показаните по-горе оценки са общи за всички общини от съответната категория.

Налице са значителни разлики в подходите на различните общини в отговор на киберзаплахи: степента на развитие на системите за МИС; поддържането в актуално състояние на документите свързани с МИС; в процесите по управление на риска; при спазване на изискванията за конфигуриране; при управлението на инциденти; при наличието на планове за непрекъсваемост и др. Разликите варират значително независимо от наличието на общи и единни критерии, които биха могли улесняват методологично надеждно, съществено сравнение. Така например най-високата и най-ниската оценка за община във всяка една от трите категории са както следва: първа категория – „много добър 5.36“ и „добър 4.12“; втора категория – „много добър 5.36“ и „удовлетворителен 2.93“; трета категория – „отличен 5.72“ и „слаб 2.48“.

Тези разлики може да се обяснява със следното:

Условията, в които работи всяка община; изисквания, продиктувани от естеството на съхраняваните данни; ниво на разбиране и приоритета, даден на МИС от тяхното ръководство; степента на осигуряване на необходимите ресурси; както и голямо разнообразие от ИКТ системи, инструменти и софтуерни решения, използвани в цялата система, често отразяващи години неkoordinирани инвестиционни решения и избор на доставчици на услуги за ИКС, въпреки структурните и други прилики, които без съмнение присъстват в много, ако не във всички общини предмет на изследването. Водеща причина за съществената разлика в оценките между общините (особено между тези от трета категория) според екипа е степента на ангажираност на ръководствата на съответните общини.

3.ЗАКЛЮЧЕНИЕ

В заключение екипът счита, че в резултат на казаното по-горе и предвид цялостната информация придобита в процеса на изследване, по степента на имплементиране на НМИМИС в общините включително и тази придобита по време на проведените фокус група и интервю може да се направи обобщение, по-важното от което е:

1. **Степен на имплементиране на изискванията на НМИМИС** – Независимо от субективните проблеми с интерпретацията на получените отговори, при наличието на обща референтна система, анализът предоставя общата сумарна картина на състоянието на МИС в изследваните общини. Тя обаче не дава основание да се смята, че в системата на 16-те общини (особено в две от общините трета категория), като цяло състоянието на МИС е безпроблемно.

Екипът обръща внимание на кметовете на изследваните общини, че установените пропуски в прилагането на НМИМИС, означава неизпълнение от тяхна страна на изискванията на Закона за киберсигурност, по чл. 21, ал. 2, т. 3.

В тази връзка екипът е направил в настоящия анализ както следва: препоръки към общини първа категория, 24 бр., препоръки към общини втора категория 36 бр. и препоръки към общини трета категория 46 бр. Тук следва да се има предвид предприемане на мерки за прилагане изискванията на НМИМИС, в съответствие със ЗКС.

2. **Ангажираност на ръководствата с постигане на високо ниво на МИС в общините** – В светлината на по-широките аспекти на МИС както е дефинирана в този анализ, екипът смята, че ръководствата на общини трябва да обърнат по-сериозно внимание на повишаване нивото на МИС. Част от всеобхватна поддръжка, която следва те да осигуряват, е да **дават стратегически насоки за това**, на управленско ниво, включително чрез изготвяне на документ, който ясно определя допустимите граници риск и подходящо разпределение на общинските ресурси. Или по-общо казано, ръководството трябва да отрази как редовното докладване по проблемите на МИС от служителите по МИС да се използва за взаимодействия с тях, в границите на това, те да се считат като необходими и достатъчни, но без да се компромеира защитата на общините.

3. **Отговорността за високо ниво на МИС, не е отговорност само на ИТ служителите и на служителите по МИС** – МИС следва да е резултат от многостранен, цялостен организационен подход. Подходът трябва да обхваща всички нива на общината, включително органи за вземане на решения и управление, надзорни органи, изпълнително ръководство, оперативно или функционални структурни звена, програмни мениджъри, персонала като цяло и външни доставчици на услуги. Както по-горе беше посочено от екипа, висока устойчивост на МИС в една община също е въпрос на силна вътрешна кибер култура, която започва с внимание и приоритет, посочени от ръководство. Това изисква постоянен интерес и участие, не само на ръководството на общината а и от останалите служители в нея. Основният елемент следва да бъде насърчаването на вътрешна култура, в която уведомяване за инцидентите в МИС не се разглеждат като провал, а като отправна точка за разрешаването на инцидента.

4. **Квалифициран персонал** – Екипът смята за приоритетен въпроса за осигуряване на квалифицирани ИТ служители и служители по МИС. Резултатите от настоящия анализ, сочат, че при наличие на достатъчен по брой и с висока професионална компетентност персонал над 90% от изискванията на НМИМС, могат да бъдат изпълнени, разбира с подкрепата на Ръководствата на общините. Необходимо е общините да посрещнат бъдещи нужди от експертен опит в МИС чрез правилно планиране на човешките ресурси, особено като се има предвид, че знанията, уменията, а и способностите за справяне с рисковете и проблемите с МИС са строго специфични. Предвид общия остър недостиг на специалисти по МИС, то такива служители може да бъдат трудно привлечани и задържани.

5. **Ключова роля на служител или административно звено, отговорни за състоянието на МИС** – Резултатите от изследването недвусмислено показват, че в общини където има определен служител по МИС (особено такъв, който не е ИТ служител и изпълнява по съвместителство функции по МИС), значително по-високо ниво на МИС. Защо е важно определянето на служител по МИС да бъде съобразено и с наличието на персонал отговарящ за ИТ. Ако двете длъжности съвпадат, това може да доведе до несъответствие между ключови задачи в/за двете направления. Докато управлението на риска и МИС е основната задача за

служител по МИС, за разлика от това за въпросите на практическата дейност и икономическата ефективност, както и ефективност на обслужването, за което отговаря ИТ персонала. Потенциалният конфликт на интереси е очевиден.

6. Засилване на системните рискове за други общини поради установени проблеми в състоянието на МИС в някои от изследваните общини – В случай на успешна кибератака, нападателят може да получи администраторски права и по-дълбок достъп до информационните системи на една община. Тогава по аналогия, такъв достъп може да се използва за проникване в цифровата територия и на друга община. Злонамерено движение от една община към друга (известно още като „препращане“) също може да бъде по-трудно за откриване и спиране, тъй като може да изглежда като нормален трафик. След като получи информация за инфраструктурата на една община, хакерите могат допълнително да коригират метода на атака и да използват специално подбран набор от техники за постигане на целта си. По този начин общините, които са допуснали съществени слабости в своята система за МИС, макар и косвено, създават проблеми и на други общини. В тази насока екипът смята за полезно и препоръчва, по инициатива на изследваните общини да се създаде в рамките на Националното сдружение на общините в Р. България, неформална среда за общуване, взаимопомощ, споделяне на информация релевантна на МИС в общини, включително и известяване за новооткрити уязвимости в използваните софтуер и хардуер.

7. Киберзастраховка – Един от вариантите за повишаване на проактивната защита срещу постоянно нарастващите киберзаплахи би могъл да бъде сключване на киберзастраховка, която ще позволява да бъдат покрити щети от кибератаки, също така да се избегне необходимостта да се занимаваме с етичния аспект на въпроса относно плащането на откуп. По време на работата по анализа не е установено някоя от общините да е застрахована за кибер рискове. Киберзастраховането може да бъде ефективен инструмент за превантивно облекчаване на съответните рискове в повечето ситуации, защото би било само стратегия за частично смекчаване на последствията от кибератака, допринасяща за минимизиране на възможните финансови щети с малка печалба по отношение на намаляване на щетите за общината или нейната репутация.

Екипът изразява своята най-сърдечна благодарност на всички представители на 16 общини, които по един или друг начин подпомогнаха изготвянето на настоящия анализ, без чиято помощ той не би могъл да бъде изготвен.*9