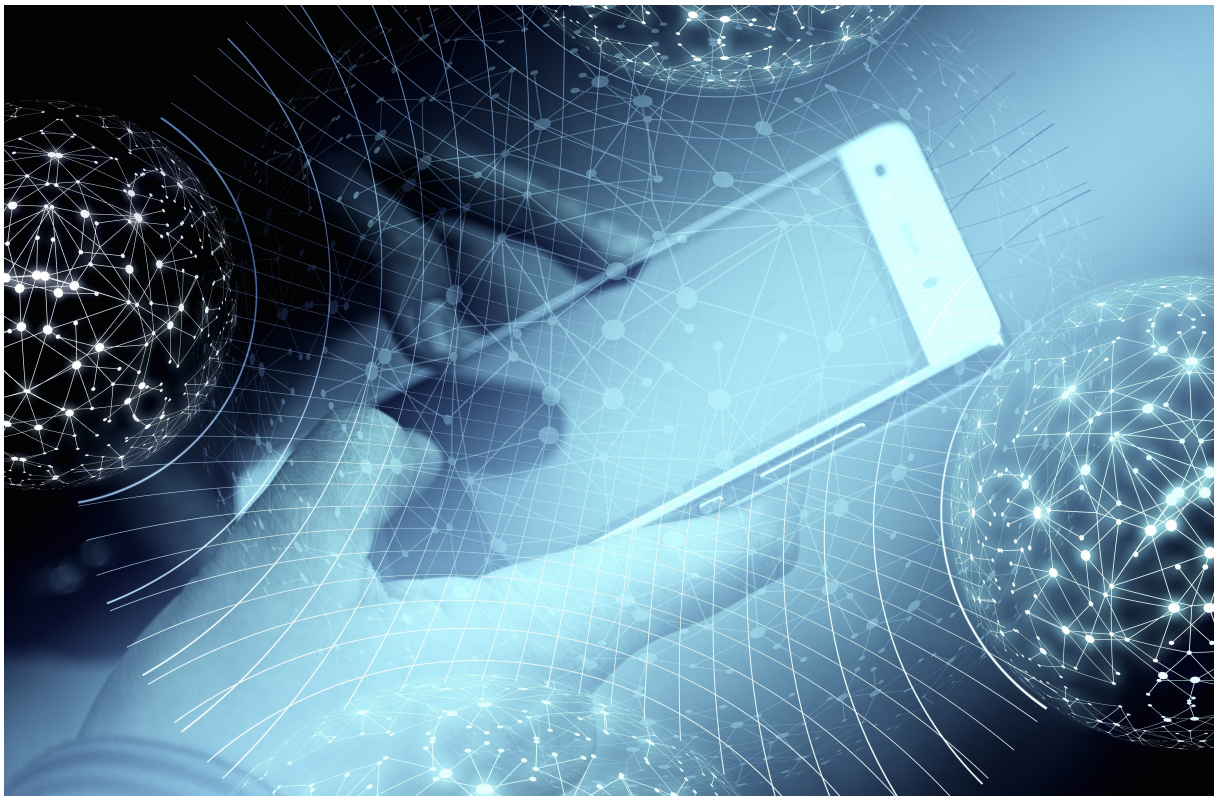
ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ
СОЦИАЛЕН ФОНД

ОПЕРАТИВНА ПРОГРАМА
ДОБРО УПРАВЛЕНИЕ

МОДЕЛ

ЗА

ИНСТИТУЦИОНАЛИЗАЦИЯ НА МЕРКИ ЗА ПОСТИГАНЕ НА ПО-ДОБРА КИБЕРСИГУРНОСТ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОБЩИНСКАТА АДМИНИСТРАЦИЯ



Юни, 2023 г.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

СЪДЪРЖАНИЕ

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

I. Въведение

Този доклад изследва препоръките на експерти в сферата на киберсигурността, за да разпише конкретни мерки, както и стъпките за тяхната институционализация в стратегическия и оперативен план на общинската администрация, за осигуряването на едно по-добро ниво на защита на личните данни и кибернетичната среда.

Дигиталната трансформация на социално-икономическите дейности и процеси, форсирана от глобалната пандемия Covid-19, направи обезпечаването на информационната и мрежова сигурност задача от първостепенно значение в стратегията на общинските администрации за устойчивост и управление на рисковете. Предизвикателство за киберзащитата се явява и законовото изискване местната власт да предоставя прозрачност и отвореност на информацията и дигиталните услуги за целите на електронното правителство. Автоматизираната обработка на данни и информация днес играе все по-ключова роля при изпълнението на функциите на администрацията. Всички основни процеси вече са поддържани от електронните и комуникационни технологии. Освен това, нормативни изисквания като Общия регламент за защита на данните (EU-GDPR), Директивата за Мрежова и информационна сигурност (МИС2) или Закона за електронното правителство, са движещи сили в прехода на публичната администрация към цифровизация. Киберсигурността се явява и ключова политика и приоритетно направление в актуализираната стратегия на Европейския съюз за е-управление 2019 - 2025г.

В тази връзка трябва да се постигне подходящо ниво на сигурност както на оперативните процеси, така и на свързаните с тях обекти на критичната инфраструктура. Под това се разбират мрежи, системи, база данни. Пробивите в тези системи, или компрометирането на масивите поверителна информация, могат да доведат до блокиране на обществени услуги и кражба на чувствителни данни. Общинските власти са особено „апетитна“ цел за киберпрестъпниците както заради количеството и качеството на информацията, с която боравят (имуществени и данъчни регистри, поверителни лични данни; избирателни списъци и др.), така и поради факта, че за разлика от частния бизнес те се възприемат, по дефиниция, за по-слабо подготвени в защитата си от кибератака. Структурите на общинската власт

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

се определят като сравнително лесна "мишена" за хакерите, поради уязвимостта на мрежовите си системи и контрола над базата данни. Публичната администрация, обикновено, разполага с ограничен ресурс за изграждане и надграждане на мрежи, контроли и системи за сигурност и може да не разполага със специализиран ИТ персонал за прилагане на организационни мерки за превенция срещу рисковете в електронната среда.

Ползата от този доклад за общинската администрация би била в това да се запознае със специфични мерки за защита на чувствителната информация на гражданите, предложени от експерти по сигурността. Както и да се поучи от най-добрите практики за институционализация на тези мерки в оперативния и стратегически план за управление на рисковете в киберпространството. Това би способствало за изграждането на едно по-информирано разбиране за предизвикателствата на дигиталния свят и би спомогнало общинската администрация в отговорната задача да надгради съществуващите си план и стратегия, за да осигури максимално ефективна защита за поверителните данни на своите граждани. Комплексността на информационните технологии, цифровата трансформация на работния процес, както и зависимостта на администрацията от непрекъснато актуализиращи и допълващи се нормативни актове в сферата на компютърните технологии, доведе до разбирането, че киберсигурността трябва да получи по-висок приоритет в стратегията за устойчивост и управление на рисковете на местно ниво.

II. Предизвикателства пред институционализацията на мерки за осигуряването на защита в кибернетичното пространство

Преди да разгледаме конкретни мерки за защита на личните данни и киберсигурността, предложени от експерти, и да изследваме най-добрите практики за тяхното институционализиране, трябва първо да се запознаем с предизвикателствата на средата. Това е ключово условие за по-доброто разбиране на проблема.

При имплементирането на оперативни и стратегически подходи за киберсигурност, публичната администрация е изправена пред няколко основни предизвикателства, с които трябва да се справи, а именно:

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

ограничени бюджетни и кадрови ресурси; комплексна ИТ инфраструктура; съответствие с регулаторни разпоредби и непрекъснатата им актуализация; човешкият фактор, като вътрешна заплахи (небрежно или злонамерено действие от служители); риск от трета страна (дистрибутори, доставчици); повишен геополитически риск (публичната администрация е основна цел на хакерски групи, тъй като е част от критичната инфраструктура на всяка една страна); бързо развиващ и усъвършенстващ се пейзаж на заплахите; липса на добра осведоменост у служителите за рисковете на киберсигурността; общественото възприятие и доверие, в случай на инцидент с поверителната информация на гражданите.

Справянето с тези предизвикателства изисква цялостен и добре планиран подход, който включва внедряването на технологични и оперативни мерки за защита, установяването на стриктни и ефективни рамки за управление, мониторинг и контрол, а също и проактивното участие в програми за обучение и повишаване на осведомеността на служителите, както и да насърчава сътрудничеството с трети страни и лица по проблемите на киберсигурността.

III. Внедряване на мерки за подобряване нивото на киберсигурност и защита на личните данни в общинската администрация

Експертите в сферата на киберзащитата се обединяват около максимата, че не е въпрос *дали* мрежите и системите на общинската власт ще станат обект на кибератака, а *кога* ще се случи това и *колко силно* ще бъде въздействието на това зловредно проникване. Такова убеждение се подкрепя и от статистиката. Европейските държави отчетоха трицифрено увеличение, в процентно измерение, на докладваните инциденти с киберсигурността по време на пандемията (Европейска агенция за киберсигурност ENISA, 2022). Изследване на ENISA показва още, че през разглеждания период най-атакуваната от киберпрестъпници сфера на обществено-социалния живот в държавите от Европейския съюз е била именно публичната администрация и правителствените учреждения.

Макар да съществуват разнородни технически и оперативни мерки, които местната власт би могла да имплементира за защита на своята поверителна

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

информация и системи, долуразписаните способи са сред най-често и настоятелно препоръчваните от експертите в сферата на киберсигурността. Те се приемат за стандарт в превенцията на широк набор от киберзаплахи като, например, вируси, зловреден софтуер, фишинг атаки, социален инженеринг и неоторизиран достъп до чувствителни данни и пароли.

Важно е да се отбележи, че нито една от долупосочените мерки не може да защити самостоятелно и/или напълно дигиталната и цифрова мрежа на дадена организация от кибератаки. Необходимо е да се приложи комбинация от политики за създаване на стабилна екосистема по сигурността.

По тази причина експертите залагат на стратегия за „защита в дълбочина“ (Defense-in-Depth Approach). Тя, в същността си, е многопластов подход за сигурност, който включва прилагане и въвеждане на множество мерки, на различни нива, за създаване на припокриващи се защитни структури. Този подход гарантира, че ако един „контрол“ за сигурност бъде нарушен, други са на място, за да осигурят припокриваща защита. Отправната точка на въпросната холистична стратегия е в осигуряването на стабилна сигурност на периметъра, състояща се от внедряване на защитни стени, системи за ранно предупреждение и откриване на проникване, защитени уеб-шлюзове и филтри за имейл в периметъра на мрежата, за да се предотврати неоторизиран достъп и да се защити системата срещу външни заплахи. Както и внедряването на усъвършенствани решения за защита на крайната точка, включително антивирусни програми срещу злонамерен софтуер и контрол над достъпа и приложенията.

От съществено значение е всички мерки да бъдат преглеждани, надграждани и актуализирани периодично, за да се гарантира, че са “в крак с времето”, както на нормативно, така и на технологично и оперативно ниво. Трябва да се отбележи, че внедряването на мерки за киберсигурност е непрекъснат процес, тъй като е непрекъснат и процесът на еволюция на уязвимостите и заплахите в кибернетичното пространство. Те стават все по-комплексни и все по-целенасочени. Затова е задължително условие структурите на общинската власт редовно да адаптират своите мерки за сигурност спрямо най-актуалните и прецезирани подходи и стандарти за защита на мрежовата и информационна екосистема.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

Имплементирането на долупосочените мерки и препоръки, или надграждането на вече съществуващи чрез тях, е доказан в практиката способ за осигуряване на холистична и надеждна защита на личните данни и мрежовите системи.

1. Оценка на уязвимостите на системите чрез въвеждането на протокол и процес по инвентаризация и актуализация: Общинската администрация трябва да подлага на редовна и обстойна оценка своите мрежови и информационни системи за уязвимости и слаби звена. Хардуерът, софтуерът и точките за достъп до Wi-Fi мрежата са въпросните слаби звена. Оценката следва да включва инвентаризация на всички тези компоненти, за да се определят видовете им, характеристиките на функционирането и достъпа до тях, честотата на необходимите актуализации, за да се създаде по-ясна представа за рисковете за данните и оборудването. Местната власт и ИТ експертите, работещи в/за нея, трябва да възприемат най-високите стандарти за сигурност, признати от индустрията в боравенето с компонентите на информационната и мрежова екосфера. Препоръчва се редовното актуализиране на софтуера и системите от официален и легитимен източник, поне 2 пъти годишно. Организациите от публичния сектор трябва да гарантират, че целият им компютърен и дигитален набор се ъпдейтва редовно с най-новите корекции и подобрения за сигурност. Това може да помогне в огромна степен за защита срещу най-разпространените и базови уязвимости. Важно е да се напомни, че е необходим само един компютър или устройство, който не е актуализиран или защитен, за да бъде компрометирана цялата мрежа на публичната администрация. Затова важно правило е да се съблюдава за подход, базиран на целостта на изпълнението на действията по защита и превенция, а не работа “на парче”.

2. Прилагане на политика за силни пароли: Общинската администрация трябва да изисква от служителите си да прилагат стриктна политика за силни пароли, за да се гарантира максимална сигурност на техните акаунти. Това може да включва изискване паролите да са с определена дължина, да съдържат комбинация от букви, цифри и специални знаци, както и да се променят редовно. Експертите препоръчват паролите да се променят на всеки 30/60 дни, като това да не става пожелателно, а да е системно изискване на софтуера и програмите, които администрацията използва.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

Друга добра практика е налагането на строги "таймаути" на работната сесия, така че ако потребителят остави включен акаунт или приложение без надзор за определен период от време, сесията автоматично да бъде прекратена. Повторното влизане ще изисква да се въведе отново потребителското име и парола. Всички компютърни устройства, системи и служебни телефони на публичната администрация трябва да имат функция за блокиране, която след определен брой невалидни/грешни опити за въвеждане на парола да блокира акаунта. Това ще позволи да се минимизира риска от "налучкване", метод, при който хакерите използват програми с неограничен брой комбинации, за да опитат да "налучкат" и пробият профили, които са незащитени чрез валидатор за грешки. По отношение на паролите трябва също да се работи активно за повишаване степента на информираност и образованост на служителите. Често срещани и разпространени в администрацията практики, като написването на пароли върху „хвърчащи" листчета и залепването им за монитор или бюро, трябва да бъдат изначално и окончателно изкоренени, тъй като крият напълно реални и сериозни рискове за сигурността на цялата система.

3. Активиране на двуфакторно удостоверяване на идентичността:
Двуфакторното удостоверяване (2FA) добавя допълнителен слой на сигурност към онлайн акаунтите. В комбинация със силна парола това е най-базовото, но, същевременно, и най-ефективно решение на проблема с директната кражба на данни чрез пробив на акаунтите. Двуфакторното удостоверение изисква от потребителя да предостави втора форма на потвърждение на профила си в допълнение към паролата. Това обикновено е код, изпратен на телефона на потребителя, или генерирането на такъв код става посредством "токен" или специална мобилна апликация. Местните власти могат да инсталират двуфакторно приложение като Google Authenticator или Salesforce Authenticator, или да използват облачни услуги като Duo Security или PingID. Организациите от обществения сектор трябва да обмислят задължителна възможност за 2FA за защита срещу неоторизиран достъп до най-чувствителната си информация и база данни. Това е изключително икономична, достъпна и изпълнима мярка, която няма да затормози и натовари бюджета на общината, а същевременно ще окаже надеждна защита за акаунтите и поверителната информация, съдържаща се в тях.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

4. Криптиране на информацията: Общинската администрация е натоварена с отговорната задача да съхранява и да борави с поверителни държавни данни и чувствителна лична информация за гражданите. Служителите на местната власт използват различни способи, за да управляват тези данни – компютри, телефони, USB устройства, външни хард-дискове, електронна поща, чатове и други форми на цифрова комуникация. Изгубени или откраднати устройства стават честа причина за инциденти с изтичане и компрометиране на поверителни данни. И ако силни пароли и двуфакторна идентификация могат да попречат за "разбиването" на акаунти, то криптирането е още по-напредничавият способ за защита срещу неоторизиран достъп до поверителни файлове, ако устройствата бъдат загубени или откраднати, или ако съобщението/информацията бъдат прихванати от нерегламентирана трета страна.

Криптирането представлява метод за защита, при който четливият текст, документ или файл се преобразува в нечетлив код, който може да бъде прочетен само от оторизираните за достъп до него с парола или ключ за сигурност. Повечето модерни операционни системи предлагат начини за цялостно криптиране на съхранените данни, включително на цялото дисково пространство. Това е надеждна практика и ефективна мярка за защита, според експерти по сигурността. Освен това има достъпни като цена облачни решения за криптиране на хардуер и софтуер, които могат да се използват в цялата публична администрация и за всички сървъри, компютри, лаптопи и мобилни устройства.

5. Архивиране на базата данни: Създаването на архив и "бек-ъп" на информационния масив, събиран и съхраняван в мрежите и системите на публичната администрация, е най-добрият начин да се избегне загуба на данни. Това може да е от изключително значение при настъпването на нежелано събитие като атака със "зловреден софтуер" ("ransomware") или увреждане на хардуера или софтуера в следствие на пожар, кражба, природно бедствие, срив на сървърите или човешка грешка. Архивирането на данните би предпазило администрацията от огромни поражения, както и би спестило значителни средства за плащането на откуп по рансъмуер инциденти или за възстановяване на мрежите и системите.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

Архивът представлява съхранено дигитално копие на външен източник, съдържащо всички важни данни. Добра практика е архивирането да се извършва често и рутинно, както и данните да се криптират. А също така архивите да се проверяват за качество и надеждност. Препоръчва се още да архивирате в поне две копия. Едно, държано извън сградата на администрацията, и друго, на различен сървър, в случай на локална катастрофа или прекъсване.

6. Антивирусни програми: Инсталирането на антивирусни програми на компютрите на общинската администрация може значително да допринесе за предотвратяване на кибератаки. Функцията на този продукт е да открива и предупреждава превантивно за злонамерен софтуер, като сканира файлове, програми и прикачени в имейл файлове. Антивирусните програми блокират вируси, троянски коне, ransomware и шпионски софтуер, като идентифицират и поставят под „карантина“ или директно премахват от компютъра злонамерените файлове. Антивирусните програми осигуряват също защита в реално време чрез наблюдение на системните дейности и мрежовия трафик. Те могат да откриват и блокират злонамерени процеси или подозрително поведение, като опити за неоторизиран достъп или необичайни мрежови връзки. Полезни са и при работата в интернет, защото съдържат функции за уеб защита, при които сканират уебсайтове и URL адреси за потенциални заплахи. Може да блокират достъпа до злонамерени уебсайтове или да показват предупреждения, ако е известно, че даден сайт разпространява зловреден софтуер или участва във фишинг дейности. Това предпазва потребителите от неволно посещение на опасни уебсайтове, които могат да доведат до заразяване със зловреден софтуер или нарушаване на данните. Много кибератаки се инициират чрез имейл, като например опити за фишинг или доставка на „заразени“ с вирус прикачени файлове. Антивирусните програми могат да сканират входящи и изходящи имейли за подозрително съдържание и да го „маркират“ за потребителя.

Антивирусните програми позволяват също централизирано управление, което е важно и практично решение за големи структури, каквито са общинските администрации. Софтуерът разполага с централизирани конзоли за управление, което дава възможност на ИТ администраторите да наблюдават и управляват внедряването на антивирусни програми в цялата

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

организация. Това улеснява последователното прилагане на правилата, наблюдението на заплахите в реално време, навременните актуализации или промени в конфигурацията.

7. Система за откриване и предотвратяване на проникване (IDPS): Инвестицията в подобно техническо решение се отплаща, защото IDPS играе решаваща роля в защитата на системите срещу различни видове заплахи, като изпълнява следните функции:

а/ Наблюдение на трафика: IDPS следи мрежовия трафик, анализирайки пакети и потоци от данни, за да идентифицира необичайни или подозрителни дейности. Той изследва както входящия, така и изходящия трафик, търсейки модели, които показват потенциални атаки или опити за неоторизиран достъп.

б/ Идентифициране на заплахи: IDPS използва различни методи за откриване на недоброжелателни опити за проникване, на базата на кода и метаданните, както и на аномалии при анализа на поведението. Базираният на метаданните подход идентифицира и сравнява мрежовия трафик с базата данни на вече известни атаки и „маркира“ въпросната дейност като подозрителна. Друга полезна функция на IDPS е, че изпраща автоматични предупреждения и известия до ИТ администраторите, които включват подробности за естеството на атаката, засегнатите системи или потребители, както и сериозността или нивото на приоритет на събитието.

в/ Реагиране на инциденти: В допълнение към генерирането на предупреждения, IDPS може да предприеме незабавни действия, за да отговори на открити заплахи. Това може да включва блокиране или премахване на подозрителен мрежов трафик, прекратяване на връзки или изолиране на засегнатите системи за предотвратяване на по-нататъшно компрометиране.

г/ Генериране на регистрационни файлове с исторически данни: IDPS разполага също с функцията да генерира регистрационни файлове и записи на мрежови дейности и събития, предоставяйки ценна информация за ИТ отделите да анализират и разследват инциденти.

8. Привеждане на ИТ доставчиците в съответствие: Не са рядкост случаите, в които общинските администрации, поради ограничения си ресурс, и/или

капацитет да се справят сами със задачите “ин-хаус”, възлагат на външни компании и трети лица доставката към общината на ИТ услуги, в това число и обезпечаването на мрежовата и системна сигурност.

В тези случаи е задължение на местната власт да извършва адекватен и периодичен риск анализ и оценка на въздействието на всички доставчици от трети страни, които имат достъп до чувствителна информация и данни, и които взаимодействат с общинските мрежи и системи. Задължение е на общинската администрация да проверява и контролира дали външните доставчици на ИТ услуги спазват всички приложими закони и регулации за сигурност на данните. Един начин това да се постигне е чрез периодичното попълване на подробни анкети по въпросите на съответстието (т.нар “due diligence”).

Освен това, общинската власт трябва да изисква от своите доставчици на електронни услуги и продукти сертификати и надлежна документация, за да потвърди компетенциите, разрешителните и съответствието на фирмата с най-високите стандарти за осигуряване на защита в киберпространството.

Важно е да се има предвид, че при възникване на инцидент с последствия, при който по нормативна уредба се налагат санкции, общинската администрация не е със снета отговорност, ако е прехвърлила задълженията си по опазване на критичната инфраструктура, данни, мрежа и системи на външен изпълнител/доставчик на услуги.

9. Изготвяне на кризисен план за действие: Както вече споменахме в увода към разписването на мерките за защита на личните данни и мрежовата система, всеки експерт по киберсигурност ще потвърди, че въпросът не е дали дадена организация ще стане жертва на кибератака, а кога. И точно заради това всяка отговорна публична администрация трябва да бъде подготвена с кризисен план за действие, който точно и ясно да разписва ролите, мерките и сроковете за реакция.

Изготвянето и утвърждаването на план за реагиране трябва да бъде изпълнено преди евентуалния инцидент, а не постфактум. Задължение на публичната администрация е да разработи превантивно набор от последователни действия и мерки, които да се задействат и изпълнят в случай на кибератака. Целта е да се смекчат и минимизират щетите от

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

зловредното проникване, и то по начин, който да намали въздействието върху критичната, дигитална инфраструктура на общината и да ѝ позволи да се върне към обичайния си оперативен живот възможно най-бързо.

Като минимум, ефективният план трябва да разкрие в най-кратък срок всички мрежи, системи и база данни, които са били компрометирани в следствие на кибератаката. Също така, трябва да определи и степенува сериозността на инцидента, да има ясна идея към кого трябва да бъде докладван проблемът и в какъв срок, както и да определи кои са засегнатите лица или институции, към които отговорните лица по изпълнението на кризисния план да се обърнат и информират, включително и как да бъде информирано населението за това кои услуги са били засегнати и какви мерки се предприемат. Всеки кризисен план трябва да има лице или лица отговорни за имплементирането и надзора му в случай на инцидент.

10. Защита на достъпа до информацията при употреба на отдалечени устройства: За такива се считат всички електронни и комуникационни устройства, които използват системи, програми, файлове и данни извън обсега и мрежите на институцията, която е техен “собственик”/принципал.

Глобалната криза, породена от пандемията Covid-19, направи работата от разстояние “новото нормално” за голям брой служители. Съвсем очаквано, лавинообразно нарастнаха и кибератаките и пробивите в сигурността, породени от факта, че много устройства, съдържащи чувствителна информация, започнаха да се използват през незащитени мрежи, както и да се използват от лични устройства, през които да се зареждат поверителни данни или програми.

За общинската администрация е наложително да обърне внимание на тези процеси и тенденции, за да осигури адекватен протокол за управление на достъпа на всеки потребител, използващ отдалечени устройства. Според доклад на компанията за киберсигурност “Bitglass” за 2021 г. 82% от 271 анкетирани организации активно са възприели в работата си подход, който позволява на служителите използването на лични устройства или външни мрежи за съхранение, обработка и прехвърляне на чувствителна и поверителна за организацията информация. Това крие редица рискове и предизвикателства за сигурността.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

По-долу експерите по киберзащита от “Bitglass” предлагат следните добри практики, за да осигурите защитен достъп на отдалечените устройства.

а/ Обучението по сигурност за служителите може да смекчи рисковете, свързани с новия подход за работа от всяко място. Научете служителите си да не позволяват на никого да има достъп до техните компютри и информация, и да предприемат мерки, за да обезопасят чрез силна парола външната мрежа като, например, Wi-Fi, през която оперират работната си дейност, както и никога да не използват отворена Wi-Fi мрежа, без защитна парола, за работа с поверителни данни и програми.

б/ Важно е да се предложи цялостно техническо решение, което да наблюдава активността на потребителите и да осигури достъп до ресурси и поддръжка за всички потребители, които се нуждаят от това, където и да се намират. Задължително базово техническо решение за работата от разстояние е да бъде активирана VPN услуга, която да бъде поддържана от ИТ специалист, свързан с работата на публичната администрация.

11. Управление на привилегиите в мрежовите и системни акаунти: Експерите по сигурността съветват да се избягва даването на привилегирован/администраторски достъп до мрежите и системите на твърде много потребители. Предоставянето на всички привилегии на нови служители, по подразбиране, им позволява достъп до чувствителни данни, дори и това да не им е необходимо. Подобен подход увеличава риска от компрометиране и увеличава шанса на хакерите да получат достъп до поверителна информация. Злоупотребата с акаунт привилегии е водещата причина за пробив в данните според доклада за разследване на нарушения на данни от 2021 г. на американския технологичен гигант Verizon.

Много по-уместно решение е да се използва принципът за даване на най-малко привилегии. С други думи, задайте на всеки нов акаунт възможно най-малко привилегии за достъп и ги ескалирайте/увеличете, ако това се окаже необходимо за изпълнението на ежедневните работни функции. А когато достъпът до поверителни данни вече не е необходим, създайте процес за редовен одит и проверка, който на определен срок от време да тества нуждата от въпросните акаунт-привилегии и да ги премахва.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

Привилегированите потребители разполагат с всички необходими средства, за да откраднат или компрометират критично важните данни, файлове и информация, като същевременно останат незабелязани. Опитът на експертите свидетелства, че дори да имате пълно доверие на служителите си и те да не възнамеряват да действат злонамерено, техните работни навици могат неволно да причинят изтичане на информация, или да позволят на хакери да проникнат в техните акаунти. Не е изненадващо тогава, че много организации наблюдават привилегированите акаунти по-внимателно, отколкото останалите профили на служителите си. Това показва и доклада за вътрешна заплаха на "Cybersecurity Insiders" от 2021 година, според който 61% от анкетираните организации имат специален протокол за наблюдение и оценка на привилегированите акаунти.

12. Съответствие с регламента за Защита на личните данни (GDPR): С навлизането на регламента за Защита на личните данни, за органите на общинската администрация е от първостепенно значение задачата да гарантират правата за поверителност на информационните масиви, които обработват и съхраняват. Съвместимостта с GDPR помага за установяване на доверие у гражданите, демонстрира ангажимент за защита на данните и позволява избягването на големи глоби, както и увреждане на репутацията на институцията. За да осигурят ефективност и сигурност, органите на общинската администрация трябва да прилагат мерки като назначаване на длъжностно лице по защита на данните; извършване на инвентаризация и картографиране (mapping) на информационните масиви; съблюдава да информира гражданите и да получава съгласието им, по законово основание, за обработка и съхранение на техните данни; предоставяне на достъпни и прозрачни съобщения за поверителност; ефективно управление на съгласието чрез зачитане на правата на субектите на данните; прилагане на стабилни мерки за сигурност, чрез провеждане на редовно обучение на персонала, извършване на оценки на въздействието върху защитата на данните (DPIA) за високорискови дейности и поддържане на тясно сътрудничество с надзорните органи. Тези мерки допринасят за цялостен и проактивен подход към защитата на данните, насърчавайки съответствието и минимизира риска от нарушаване на сигурността на данните или нарушаване на поверителността.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

В обобщение, киберсигурността продължава да представлява значително предизвикателство за всички нива на общинската администрация, но тя може да си послужи от опита и експертизата на ИТ индустрията, която, по дефиниция, се адаптира по-лесно и по-бързо към еволюцията на рисковете, заплахите и способите за превенцията им. Специалистите по сигурността създават множество възможности за предоставяне на нови услуги и продукти, които да се използват за обезпечаване на високи нива на защита за общинската власт, нейните мрежи, данни и системи.

В имплементирането на мерки, продукти и услуги за сигурност, общинската администрация трябва да бъде проактивната страна: да насърчава сътрудничеството с частния сектор, академичните среди, националните органи и гражданското общество за повишаване осведомеността и компетентността на гражданите и служителите в сферата на дигиталните технологии и за целите на разработването и внедряването на ефективни политики по киберсигурност. Такива, които да са "в крак с времето", технологично и нормативно; да изграждат обществено доверие в системата и да оказват въздействие към цялостното подобряване на екосистемата за превенция от кибернетични инциденти.

IV. План за институционализация на мерките за постигане на по-добра киберсигурност в общинската администрация

Разработването и имплементирането на план за превенция на зловредното проникване в мрежовата и информационна система на публичната администрация включва холистичен, стратегически подход за защита на чувствителните данни и на критичната инфраструктура. По-долу ще разгледаме, стъпка по стъпка, практиката за институционализация на стратегията по киберсигурност, като поставим акцент върху възможните пречки, както и начините рисковете да бъдат минимизирани.

Прилагането на подобен план за действие изисква внимателно планиране, координация и постоянна бдителност за динамиката на промените.

Стъпка 1: Създайте вътрешна структура (административно звено) за управление на рисковете по киберсигурността. Сформирайте специализиран екип, който да отговаря за стратегията, прецизирането ѝ,

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

изпълнението и надзора върху плана за защита на личните данни и информационните мрежи на общинската власт. Определете ролите и разпределете отговорностите на всеки един служител в рамките на звеното за киберсигурност. Обезпечете го ресурсно, както финансово, така и чрез експерти с допълваща се техническа и оперативна компетентност.

Потенциални пречки: Създаването и поддържането на специализирано, експертно звено по киберсигурност ще бъде ресурсоемко начинание за всяка общинска власт. Друг потенциален проблем би се породил при неясно и неточно разпределение на ролите и отговорностите по изпълнение на задачите, както и при активирането на кризисния план за действие в случай на инцидент свързан със зловредно проникване в системите и мрежите на общинските сървъри. Рискът е, при непрецизиране на „собствеността“ върху стъпките по имплементирането на плана за киберзащита, отговорностите да се размиват или дублират, което да доведе до неефективност в изпълнението.

Смекчаване на риска от неефективно прилагане: По въпроса с ресурсното обезпечаване на звеното, потърсете (съ)финансиране от националния бюджет, както и по европейски програми. Бъдете проактивни в търсенето на публично-частни партньорства с бизнеса, академичните среди, гражданското общество, откъдето може да почерпите опит и експертиза, както на техническо, така и на кадрово и оперативно ниво. Подобни партньорства могат да бъдат не само по-икономични решения, от гледна точка на общинския бюджет, но и да привлекат външна експертиза, която липсва при едно изцяло „ин-хаус“ изпълнение на заданието. За да смекчите риска от неефективно прилагане на стъпката, дефинирайте ясно отговорностите на всяка роля от самото начало, и осигурете редовна комуникация и сътрудничество, както между хората в екипа, така и с всички останали трети страни, имащи участие и касателство в изпълнението на плана по защита на личните данни и на мрежовата сигурност.

Стъпка 2: Извършете цялостна, подробна оценка на риска и въздействието. Идентифицирайте, картографирайте и категоризирайте всички потенциални рискове за киберсигурността, свързани с поверителността на данните и на уязвимостите на информационните и мрежови системи, специфични за вашата организация. Оценете въздействието и вероятността

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

от всеки риск, за да приоритизирате усилията за смекчаване и да насочите правилните ресурси в правилната посока.

Потенциални пречки: Неадекватната оценка на риска може да доведе до непълно разбиране на уязвимостите и заплахите, което да доведе до неефективни стратегии за смекчаване на вредите при евентуално настъпване на неблагоприятно събитие. В същия смисъл, неправилното разбиране и приоритизиране на рисковете и заплахите може да отклони ресурси и навременни усилия в разработването на правилните технически и оперативни методи за предотвратяване на сериозен киберинцидент.

Смекчаване на риска от неефективно прилагане: Ангажирайте външни експерти или консултанти по киберсигурност, които да ви помогнат при извършването на задълбочен анализ на риска и въздействието. Редовно актуализирайте оценката и се консултирайте със специалисти от ИТ сферата, за да се справите с динамиката и комплексността на непрестанно еволюиращите заплахи и промени в кибернетичния пейзаж.

Стъпка 3: Разработете подробен план за действие на база констатациите от оценката на риска и въздействието. Този план следва да очертава конкретни мерки и инициативи, които да бъдат приложени в определен срок, и с определена степен на приоритетност, за да се минимизират рисковете и заплахите от евентуално зловредно проникване в мрежата и системите на общинските компютри и сървъри. Ясно дефинирайте целите на всяко действие, за да осигурите яснота и съответствие с целите на организацията.

Например, целите могат да включват повишаване на сигурността на мрежата, подобряване на възможностите за реагиране при инциденти или повишаване на информираността на служителите. Разбийте всяка цел на конкретни стъпки за действие. Например, ако целта е да се подобри сигурността на мрежата, стъпките за действие могат да включват внедряване на защитна стена от следващо поколение, провеждане на редовни оценки на уязвимостта и въвеждане на системи за откриване на проникване. Идентифицирайте лицата или екипите, отговорни за изпълнението на всяка стъпка на действие. Възлагането на ясни отговорности гарантира отчетност и улеснява гладкото изпълнение. Установете реалистични срокове за всяка стъпка на действие, за да следите

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

и контролирате напредъка. Вземете под внимание специфични нормативни и регулаторни изисквания, като тези, посочени в GDPR или други приложими разпоредби за защита на данните. Уверете се, че планът за действие е в съответствие с тези изисквания. Създайте механизми за наблюдение и проследяване на напредъка на плана за изпълнение. Редовно преглеждайте състоянието на всяка стъпка на действие, оценявайте всички предизвикателства или забавяния и правете необходимите корекции, за да осигурите навременно изпълнение. Периодично преглеждайте и актуализирайте плана, за да отразите промените в ландшафта на заплахите, технологичните изменения или вашите вътрешни приоритети.

Потенциални пречки: Разработването на прекалено сложен или нереалистичен план за действие може да попречи на успешното му изпълнение. Както и на план, който не е съобразен с възможностите и ресурсите, и не е базиран на резултатите от оценката на риска и въздействието.

Смекчаване на риска от неефективно прилагане: Поддържайте плана за действие фокусиран, постижим и съобразен с възможностите и ресурсите на организацията. Разделете го на управляеми фази, за да улесните изпълнението и проследяването на напредъка. Фокусирайте се първо върху областите с висок риск, за да смекчите най-критичните уязвимости. За онези мерки или стъпки, за които не разполагате с налични ресурси или знания, помислете за начин да потърсите помощ, съвет или подкрепа от трети страни (гражданско общество, академични среди, ИТ сектор).

Стъпка 4: Внедряване на нови и/или надграждане на съществуващите технически и процедурни контроли за осигуряване на надеждна защита на мрежите и базата данни. Разработете конкретен план за имплементирането на въпросните технически решения, като го обвържете с конкретни срокове, планирате финансовата им обезпеченост и определите ниво на приоритетност. Примерен план може да включва следните компоненти:

Конфигурирайте защитни стени и системи за откриване и предотвратяване на проникване (IDPS), както в периметъра на мрежата, така и на външните устройства, за да наложите правила за достъп, да блокирате опити за неоторизиран вход, за да засичате аномалии и за да наблюдавате и

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

контролирате входящия и изходящия трафик. Внедрете механизми за многофакторно удостоверение (MFA), за да гарантирате, че само оторизирани лица имат достъп до системи и данни. Наложете принципа на най-малкото привилегии (PoLP), като предоставите на потребителите минималното ниво на достъп, необходимо за изпълнение на техните задачи. Приложете криптиране на чувствителни данни и архивиране на важна информация на външни, защитени източници. Създайте устойчив процес по актуализация и корекции, за да гарантирате, че софтуерът, операционните системи и фърмуерът са актуални с най-новите ъпдейти за сигурност. Внедрете инструменти и системи за наблюдение на сигурността (SIEM), за да получавате навременна информация за мрежовите и системни регистрационни файлове, по отношение на подозрителни дейности или потенциални инциденти със сигурността.

Потенциални пречки: Ненавременно, неправилно или непремерено внедрените и конфигурирани контроли за сигурност могат да донесат нови уязвимости или да причинят оперативни смущения. Много от тях ще изискват обучение на служителите, както и финансов ресурс за закупуване и внедряване на технологичния продукт.

Смекчаване на риска от неефективно прилагане: Ангажирайте професионалисти по киберсигурност, за да осигурите правилната конфигурация и прилагане на контролите за сигурност. Редовно тествайте и наблюдавайте ефективността на контролите и незабавно адресирайте всички проблеми. Инвестирайте в план за обучение на служителите и за повишаване на компетенцията им по въпроса с технологичните решения. Потърсете финансова подкрепа от бизнеса, националния бюджет или европейско финансиране.

Стъпка 5: Разработете кризисен план за реагиране, който очертава стъпките, които трябва да се предприемат в случай на инцидент с киберсигурността. Определете роли, отговорности, комуникационни протоколи и координиран подход към управлението на инциденти, с фокус към бързото възстановяване на мрежите, системите и информационните масиви. Създайте кризисен екип, в който да са включени хора с разнородни компетентности. Възложете конкретни задачи и роли, като например координатор по инцидентите, технически ръководител, комуникационен и

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

ПР отговорник, правист, технически анализатор. Създайте канали на комуникация за докладване на инциденти и координация при възникнал проблем. Приложете процедури за ограничаване на инцидента, за да предотвратите по-нататъшни щети или неоторизиран достъп и да минимизирате степента на зловредно проникване, ако такова възникне. Разработете и имплементирайте процедура за бързо възстановяване на засегнатите системи и връщане към нормалните операции след възникването на проблем.

Потенциални пречки: Липсата на адекватни процедури за реагиране при инциденти, както и липсата на кризисен екип с ясно дефинирани роли и отговорности, могат да доведат до забавяне на откриването, ограничаване на въздействието и възстановяването след инциденти.

Смекчаване на риска от неефективно прилагане: Редовно тествайте и актуализирайте плана си за реакция при инцидент чрез симулация на инциденти. Обучете служителите за техните роли и отговорности, и анализирайте резултатите от реакцията при минали инциденти, за да идентифицирате области за подобрение.

Стъпка 6: Повишете компетентността на служителите си в сферата на киберсигурността, като инвестирате в програми и обучение. Служителите са най-важната защитна преграда за една администрация пред заплахите за информационната и мрежова система и базата данни. Повишаване на тяхната компетентност и осведоменост пред рисковете, както и обучение за това как да се справят с най-разпространените видове измами и атаки, като фишинг измамите, е от ключово значение за изграждането на една цялостна среда на сигурност в структурите на местната власт.

Потенциални пречки: Основен проблем пред надграждането и разширяването на тези обучителни програми, както и пред инвестирането в напредничави технически продукти и услуги за защита, се явява ограниченият ресурс на общината за подобни дейности.

Смекчаване на риска от неефективно прилагане: За да се справи с това, общинската власт може да кандидатства за финансиране чрез безвъзмездни средства на европейско ниво, както и чрез сключването на партньорства с

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

външни организации от частния сектор (ИТ компании, университети, граждански организации).

Стъпка 7: Редовна оценка на състоянието на киберсигурността. Внедрете система за мониторинг, базирана на индикатори, които да извършват непрекъснато проследяване и анализиране на входната и изходна точка на периметъра, така че събраните данни да служат за оценка на състоянието на информационната и мрежова система. Подлагайте на редовен анализ ефективността на въведените контроли и преглеждайте състоянието на киберсигурността на организацията. Това включва внедряване на инструменти за наблюдение на информационните масиви, извършване на оценки на уязвимостта и тестове за проникване, установяване на бенчмарк показатели и извършване на одити и оценки на сигурността. Важно е да бъдат анализирани и поуките от минали инциденти, и да се използват заключенията от тях, за да се подобрят мерките за сигурност и да се актуализират протоколите.

Потенциални пречки: Пренебрегването на редовната оценка на състоянието на киберсигурността може да доведе до неоткрити уязвимости и до измамното чувство за сигурност. Най-честата причина това да се случва е поради относително високите разходи и кадрови ресурс, който е необходим, за да се извършват непрекъснати и детайлни проучвания, тестове, оценки и анализи.

Смекчаване на риска от неефективно прилагане: Това може да се постигне чрез проактивни действия и насърчаване на сътрудничество между местните власти и частния сектор в разработването и въвеждането в употреба на иновативни продукти и услуги в сферата на ИТ сигурността. Информационната и мрежова система на общинските власти е особено уязвима на хакерски атаки и местната власт и ИТ сектора могат да си бъдат взаимно полезни в това да бъдат изпробвани най-новите методи за ИТ мониторинг, контрол и анализ в реална обстановка.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

V. 10 препоръки за изграждането на успешна стратегия по киберсигурност и защита на личните данни в общинската администрация

При разработването на правилна стратегия за борба с киберсигурността, и с цел да се постигне максимална ефективност на приложените мерки, общинската администрация може да се възползва от следните препоръки за преформулиране на своята политика:

1. Приложете ориентиран към хората подход за сигурността: Служителите могат да бъдат както най-големия риск за сигурността на една общинска администрация, така и нейната най-силна защита. В днешно време технологичният подход към киберсигурността не е достатъчен, за да осигури цялостната превенция, тъй като хакерите често използват служителите/потребителите като "входна точка". Ето защо е най-добре да използвате ориентиран към хората подход за смекчаване на рисковете, свързани с киберсигурността.

Първият и най-важен съвет на специалистите е да се осъществи една честна и открита комуникация с всички служители за тяхната функция и значение в този процес. Ключово условие е те да разберат и възприемат защо спазването на правилата за киберзащита е толкова важно. Доклад на компанията за киберсигурност "Ponemon" разкрива, че през 2021 година 62% от всички пробиви на база данни са причинени от грешки или небрежност от страна на служителите на частни или публични организации. Затова е от решаващо значение на същите да се обясни, че действията им, както и, респективно, бездействията водят до определен резултат и имат цена. Всеки един от тях трябва да премине минимум базово обучение по киберзащита; да му бъдат показани реални примери от ежедневието и последствията от тях, както и да бъде обучен за това какви мерки и способи да възприеме в работата си, за да ограничи до минимум възможността за настъпване на нежелан инцидент в киберпространството.

Пример за добри практики в повишаването на осведомеността на служителите за рисковете в кибернетичната среда е организирането на "уъркшоп" за най-популярните техники за "фишинг" и най-добрите начини потребителите да ги забележат и отбягват. В допълнение на това, добра

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

практика е ИТ специалистите, работещи за дадена общинска администрация, да програмират и конфигурират "спам"-филтъра за по-голяма степен на сигурност така, че най-очевидните спам имейли да бъдат винаги автоматично блокирани.

Експертите в сигурността се обединяват около мнението, че когато дадена организация инвестира в отношенията си със служителите и ги представя като част от решението, като партньор в защитата на сигурността, случаите на небрежност и грешки намаляват и хората се отнасят по-отговорно към общи цели и каузи.

2. Да познава добре спецификите на своята среда: Всяка местна власт е до известна степен уникална по отношение на потенциалното въздействие от различните видове рискове. Добрата стратегия и добрата отправна точка за планиране се състоят в детайлното и правилно разбиране на именно тези специфики. Прилагането на универсален подход за киберсигурност има преимуществата на това, че се базира на най-добрите и актуални практики и съвети от страна на експертите, но рискува да пропусне уникалния оперативен контекст на вашата организация и среда, включително инфраструктура, системи, процеси и база данни. Разбирането на тези специфики е от съществено значение за идентифициране на потенциални уязвимости и разработване на персонализирани мерки за сигурност, които са в съответствие с оперативните изисквания на самата организация, в случая – общинската власт. Публичната администрация не трябва да гледа на киберсигурността единствено през призмата на ИТ проблем. Нито да мисли за нея като за заплаха, която може да бъде отстранена само от сбор от технически способи и компетентности. Киберсигурността трябва да се разглежда като споделена отговорност на цялата структура, изискваща подход отгоре-надолу ("top to bottom)", започвайки от кмета и общинските съветници и достигаща до всички останали служители. Всеки трябва да е наясно с рисковете и отговорностите, които произтичат и се носят, за да се гарантира сигурността на личната информация и поверителните данни.

Да сте добре запознати със спецификата на средата, преди да приложите план за действие по киберсигурността, е от първостепенно значение за оперативната ефективност и стратегическото привеждане в съответствие на въпросния план. Това позволява персонализиран подход към мерките за

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

сигурност, включващ ефективното разпределение на ресурсите, спазването на нормативните и регулаторни изисквания, правилното планиране на непрекъснатостта на дейността в случай на инцидент, както и ангажирането на всички отговорни и/или заинтересовани страни по темата защита на личните данни и киберсигурността.

3. Изгответе план за изпълнение: Една стратегия може да бъде само толкова ефективна, колкото е успешно нейното прилагане. Следователно, ефективното прилагане на стратегията по киберсигурност зависи изцяло от приемането на план за действие, който да преведе стратегията до конкретни дейности и политики чрез координиране на усилията и ресурсите.

Планът за изпълнение трябва също така да включва създаването на ясен механизъм за докладване на инциденти, и на екип за реагиране и координиране на управлението на тези инциденти, с функции както вътре, в самата мрежова и информационна система на общината, така и с правомощия да комуникира и сътрудничи с национални органи и частни субекти от ИТ сферата. Докладването на инциденти с компютърната сигурност от местните власти към националните органи играе съществена роля за подобряване и на националната киберсигурност като цяло. Подобно докладване допринася за коригиране и приспособяване на списъка с мерки за киберзащита към променящия се пейзаж на заплахите.

Планът за изпълнение трябва да включва и разработването на ключови индикатори за наблюдение и оценка на успеха на стратегията и дали тя се изпълнява в съответствие с разписаните цели, приоритети и срокове. Същите трябва да се анализират редовно, за да се провери дали не е необходима калибрация, промяна на фокуса или отпускането на допълнителни ресурси за обезпечаването на поставените цели. Предхождаща разработването на ключовите индикатори трябва да е дейността по подробен анализ на съществуващата киберекосистема на дадената община от ИТ специалист по киберсигурност, който да даде насоки за уязвимостите на средата, към чието подобрение да бъдат насочени мерките в стратегията.

Чрез конкретни и систематизирани мерки, добре разработеният план за действие се фокусира върху адресирането на идентифицираните рискове и

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

уязвимости, и прилагането на ефективни контроли за смекчаване на рисковете и въздействието от евентуални пробиви в сигурността.

Планът за действие помага също за ефективното разпределяне и управление на ресурсите. Това е особено валидно за структурите на общинската власт по места, които разполагат с твърде ограничен финансов и човешки капацитет за управление рисковете по киберсигурността. Добре разработеният план за действие идентифицира необходимите ресурси, като бюджет, персонал и технологии, необходими за прилагане на стратегията за киберсигурност. Чрез ясно дефиниране на нуждите и приоритетите от ресурси, организацията може да ги разпредели по-ефективно и да оптимизира тяхното използване за максимално въздействие. А също и да направи правилните анализи, за да потърси помощ и подкрепа „отвън“ – чрез публично-частни партньорства, от ИТ сектора или гражданското общество, като по този начин още насърчава комуникацията, сътрудничеството и споделянето на знания, повишавайки общата ефективност на стратегията за киберсигурност за гражданите и обществеността.

4. Да формулира и обясни ясно целите и задачите: При разработването на всеобхватна киберстратегия е важно визията и целите ѝ да бъдат правилно и ясно формулирани и още по-точно и ясно обяснени на всички субекти, които ще бъдат ангажирани с дейности в сферата на киберзащитата на публичната администрация. Успехът на стратегията зависи от степента на възприятие и разбиране, тъй като човешкият фактор и неговите действия или бездействия в киберпространството си остават най-ключовият фактор в борбата с киберпрестъпността. С други думи, ако общинската администрация не предприеме необходимите усилия да разясни на своите служители защо изпълнението на стратегията и мерките, заложени в нея, са от първостепенна важност, тя най-вероятно няма да пожъне успеха, на който се е надявала.

Тези своеобразни разяснителни семинари трябва да включват и график за обучение на служителите, целящо да повиши осведомеността им относно рисковете и заплахите в киберпространството. Инвестирането в повишаване компетентността на служителите е основополагащо, за да се гарантира, че отделният потребител знае как да се защити от зловредните практики в дигиталната среда, които, потенциално, могат да засегнат не

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

само публичната администрация по места, а и националната киберсигурност на цялата държава.

5. Киберсигурността не е задължение на един човек: Императив на всяка стратегия за защита на личните данни и информационната и мрежова система трябва да бъде убеждението, че киберсигурността е обща отговорност. Тя не е отговорност на една регулаторна агенция, на една частна/публична организация или на физическо лице, а е споделена от всички, свързани с интернет или използващи приложения, които са налични в дигиталната среда. Успешните кампании за повишаване на осведомеността подпомагат предаването на знания, които са лесни за разбиране и специфични за целта. Те могат да бъдат планирани и изпълнени в сътрудничество с всички заинтересовани страни, включващи държавни служители, частни компании като: доставчици на интернет услуги, телекомуникационни компании и др., както и граждански организации като: неправителствени организации, медии и академични среди.

Култивирането на една цялостна екосистема от субекти и обекти със сходно ниво на компетентност в областта на киберсигурността задължително ще доведе до ползотворни резултати, изразяващи се в по-добре подготвена и защитена среда от рисковете на киберпространството. Инвестирането в повишаването на компетентността и осведомеността на служителите за рисковете в кибернетичното пространство е най-надеждният и препоръчван метод за предотвратяване на нови киберинциденти. Наличието на добре информирана и компетентна работна сила, която разбира рисковете на киберпространството, спомага за намаляване на риска от човешка грешка, която е най-често срещаната причина за инциденти, свързани със сигурността. Например служител, който е наясно с опасностите от отваряне на подозрителни линкове или прикачени файлове, е по-малко вероятно да стане жертва на фишинг измама. Освен това, когато инвестирате в киберзнанията и уменията на вашите служители, е по-вероятно те да поемат лична отговорност по темата на киберсигурността за своята администрация/отдел и да бъдат по-отдадени и бдителни в тази си функция.

6. Гражданско участие, публично-частно партньорство и сътрудничество: Гражданското участие в диалога, формулирането на политиките на

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

публичната власт и осъществяването на контрол върху изпълнението им е една от най-висшите характеристики и фундаментален аспект на демократичното управление. Той е залегнал както в българската конституция, така и в Хартата на Европейския съюз за основните човешки права, а също и в редица нормативни актове, които регулират правата и задълженията на местното самоуправление и гражданското общество. В този смисъл не е пожелателна практика, а задължение на общинската власт.

Степента на активност и ангажираност е индикатор за зрелостта на едно гражданско общество. Голямата отговорност да култивира и поддържа среда на прозрачност, достъпност, информираност и взаимодействие с гражданите по въпроси с обществена значимост се пада на местната власт, тъй като тя е най-близо до нуждите и проблемите на населението. Участието на гражданите, под различна форма, в диалога по киберсигурността на общинската администрация изглежда задължителен, като се има предвид, че общинската власт борави с личните данни и чувствителната, поверителна информация именно на своите граждани.

Инвестирането на време и ресурс в комуникация и партньорство с гражданите, академичната среда и частния ИТ сектор позволяват достъп до знания, информация, продукти и услуги, които не са налични „ин-хаус“. Освен това публично-частното сътрудничество е важно за защитата на критичната инфраструктура на мрежите и системите, тъй като по-голямата част от нея се притежава и управлява именно от частни субекти. Диалогът с гражданите пък позволява на общинските органи да оценят ефективността на своите политики и услуги, както и, евентуално, да направят навременни корекции, след като са се вслушали в мнението, нуждите и опасенията на гражданите. Колкото по-достъпна и прозрачна е комуникацията в двете посоки, толкова повече властта се приближава до хората и печели тяхното доверие, признание, разбиране и повишава чувството за ангажираност и обща кауза. Това може да се случи на тематични срещи по киберсигурност, ден на отворените врати, кръгли маси и прочие.

7. Провеждайте редовни одити на киберсигурността: Навременният анализ на метаданните за съмнителни и нерегулярни дейности от страна на служители, привилегировани потребители или външни доставчици на ИТ

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

услуги е от ключово значение за превантивното справяне с инциденти. Качеството на одита зависи от пълнотата на данните, събрани по различни начини и методи, и от различни източници: регистрационни файлове, записи на сесии, метаданни, докладване от служители и т.н. Това е ключова мярка в управлението на въздействието от киберинцидент, затова я направете приоритетна ос в стратегията си и ангажирайте необходимия ресурс, финансов и кадрови, за изпълнението ѝ. По-добре е да инвестирате средства в превенция и одити за по-добро разбиране на рисковете, отколкото многократно повече за отстраняването на евентуалните щети.

Организациите получават до 40% от данните за поведението на потребителите си от регистрационните файлове на сървъра, според проучване на “Cybersecurity Insiders” от 2021 г. Те получават още 30% от данните чрез анализ на поведението на потребителите или от доклади на служители, според същото изследване. Подробните регистрационни файлове за сигурност предоставят информация както за дейността на крайните потребители, така и за привилегированите потребители: метаданни за активността, екранни снимки и други подробности. Тази информация ви помага да извършите анализ на първопричината за инцидент със сигурността или да идентифицирате проактивно слабите места във вашата киберсигурност. Съществуват също така автоматизирани отчети за определени видове действия, инциденти, потребители и т.н., които макар да изискват допълнителен ресурс, биха помагнали значително, за да ускорят и опростят вашите одити. А те са от изключително значение за поддържането на здравословна и защитена киберсреда.

8. Опростете технологичната инфраструктура: Ако инфраструктурата за киберсигурност на вашата администрация е насочена към намаляване на риска от пробиви на данни, тогава тя не трябва да съдържа твърде много части и да бъде разделена между много страни, осигуряващи я с различни услуги/решения. Твърде многото инструменти за киберсигурност могат да затруднят откриването и предотвратяването на заплахи. Това е така, защото внедряването на много инструменти за сигурност и включването на голям брой субекти и обекти в системата за защита имат няколко съществени недостатъка.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

Първо, рискът различните доставчици на услуги да поддържат различно ниво и качество на отчетността, което да затрудни евентуални разследвания на инциденти. Второ, може да бъде много скъпо да внедрите и управлявате нови решения в една вече съществуваща комплексна инфраструктура и това да усложни правилното управление на сигурността. Ако искате също така да намалите разходите си и времето за реакция, както и да подобрите ефективността на процеса, уверете се, че вашето решение е интегрирано с всички инструменти, от които се нуждаете: наблюдение на активността, откриване и предотвратяване на заплахи, анализ и управление на достъпа. Помислете за цялостно решение, което съдържа цялата необходима функционалност. По този начин ще рационализирате и опростите вашата инфраструктура за сигурност.

9. Бъдете в крак с най-новите регулаторни промени и разпоредби в областта на киберсигурността: Законодателството в областта на защитата на мрежовите и информационни системи се развива, актуализира и подменя непрекъснато, защото винаги се явява догонващо в играта на "котка и мишка" спрямо все по-иновативните и комплексни подходи за кибератаки, които хакерите разработват и възприемат. Затова е важно и необходимо общинската администрация да бъде в крак с най-новите разработки, доклади и препоръки и да разполага с отговорно лице, което да съблюдава и докладва навременно за промени в регулаторната и нормативна база. Това ще гарантира, че местната власт спазва закона и че нейните мерки за киберсигурност са винаги актуализирани до най-добрите стандарти и изисквания. Навременното следене на регулаторните актуализации и/или нововъведения е и полезно чисто от практическа гледна точка, защото често включва „наготово" съвети и насоки, свързани със защитата на данните и поверителността, спестявайки по този начин средства за ангажирането на външни консултанти по сигурността.

10. Сътрудничество с други специализирани звена по киберсигурност в общинските администрации, на национално и международно ниво: Един истински шампион по темата на киберсигурността, на общинско ниво, ще се стреми да бъде проактивен и да установи обмен на опит, знания и сътрудничество с други общински администрации със специализирани звена по киберсигурност, както на национално, така и на международно

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

равнище. Ползите от подобен тип взаимоотношения изобилстват и включват:

а/ Подобрена осведоменост: Сътрудничеството в сферата на киберсигурността между общинската администрация и други структури от общинската власт, на национално и международно ниво, позволява да се получи по-широко и по-задълбочено разбиране на развиващия се пейзаж на киберзаплахите. Помага за идентифициране на възникващи заплахи и тенденции, позволявайки навременни и ефективни превантивни мерки.

б/ Подобрено реагиране при инциденти: Съвместните усилия за реагиране при инциденти подобряват скоростта и ефективността на действията за възстановяване и смекчават зловредното въздействие от пробив в киберсигурността. Споделените ресурси, експертен опит и координация позволяват унифициран отговор на инциденти с киберсигурността, минимизирайки тяхното въздействие.

в/ Ефективност на разходите: Сътрудничеството позволява на структурите на местната власт да обединяват ресурси, да споделят разходите и да използват икономии от мащаба. Това води до по-рентабилни решения за киберсигурност и по-висока възвръщаемост на инвестициите.

г/ Споделяне на знания и развитие на умения: Сътрудничеството с други структури от местното самоуправление улеснява обмена на знания и на добри практики. Създава възможности за професионално развитие и повишаване на уменията на персонала по киберсигурност чрез организирането на семинари, уъркшопове и обучения.

д/ Подобрена и засилена устойчивост на киберсигурността: Чрез сътрудничество общинските администрации могат колективно да се справят с предизвикателствата на киберсигурността и да укрепят цялостната си устойчивост. Това създава единен фронт срещу киберзаплахите и подобрява позицията на киберсигурността на публичния сектор като цяло.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

V. Заключение

Този доклад цели да дефинира подходящи технически и оперативни мерки за постигането на по-високо ниво на киберсигурност и защита на личните данни в общинската администрация. Както и да разработи модел за институционализация на тези практики, чрез предлагането на конкретни стъпки, прилагането и изпълнението на които да доведат до преформулиране и/или надграждане на съществуващите стратегия и политики на общинската власт. Предложените мерки са определяни от експертите в сферата на киберсигурността за стандарт в превенцията на широк набор от киберзаплахи като вируси, зловреден софтуер, фишинг атаки, социален инженеринг и неоторизиран достъп до чувствителни данни и пароли.

Ефективното разработване на стратегия по киберсигурност и привеждането ѝ до конкретен план за изпълнение, обвързан с цели, приоритети, мерки и срокове, е от решаващо значение за подобряване на общото ниво на киберсигурност в общинската администрация. Като възприемат проактивен и всеобхватен подход, базиран на най-добрите практики и насоки за институционализация, организациите от публичния сектор могат да подобрят способността си да защитават чувствителната и поверителна информация за гражданитеи да повишат степента на доверие в институцията.

От стратегическа гледна точка един умело разработен план за киберсигурност установява ясна рамка за управление на рисковете и тяхното въздействие. Той гарантира, че организацията е в съответствие с нормативните и регулаторни разпоредби, позовава се на най-добрите стандарти и практики за защита, може да идентифицира и анализира потенциални заплахи и уязвимости, както и да насочва ефективно ресурси за справяне с тях.

На оперативно ниво институционализирането на политики за киберсигурност включва внедряване на технически мерки, такива за мониторинг, одит и контрол на сигурността, както и образователни програми за повишаване осведомеността и компетенцията на служителите.

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център" и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg

Важно е обаче да се акцентира, че внедряването на мерки за киберсигурност е непрекъснат процес, тъй като е непрекъснат и процесът на еволюция на уязвимостите и заплахите в кибернетичното пространство. Те стават все по-комплексни и все по-целенасочени. Затова е задължително условие организациите на общинската власт редовно да адаптират своите мерки за сигурност спрямо най-актуалните и прецезирани подходи и стандарти за защита на мрежовата и информационна екосистема.

Използвани източници:

Доклади:

1. “Cybersecurity Policy Framework: A practical guide to the development of national cybersecurity policy”. Author: Kaja Ciglic, Microsoft, 2021

2. “ITAPS State Cybersecurity Principals & Best Practices”. Author: Liam Crawford, 2021

3. “15 Cybersecurity Best Practices to Prevent Cyber Attacks”. Author: EKRAN, 2022

4. "How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project". Authors: Luigi Coppolino; Salvatore D'Antonio; Giovanni Mazzeo; Luigi Romano; Luigi Sgaglione, 20189.

Уебсайтове и линкове:

https://www.crosswordcybersecurity.com

https://www.ekransystem.com/en/

https://diamatix.com/bg/добри-практики-за-киберсигурност-към/

https://learn.microsoft.com/en-us/security/compass/compass

https://www.enisa.europa.eu

Използваната снимка на корицата е “royalty-free” от сайта www.pixabay.com

Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 2014- 2020 (ОПДУ 2014-2020). Цялата отговорност за съдържанието на документа се носи от Бенефициента Фондация „Ресурсен център“ и при никакви обстоятелства не може да се приема, че този документ отразява официалното становище на Европейския съюз и Управляващия орган. www.eufunds.bg