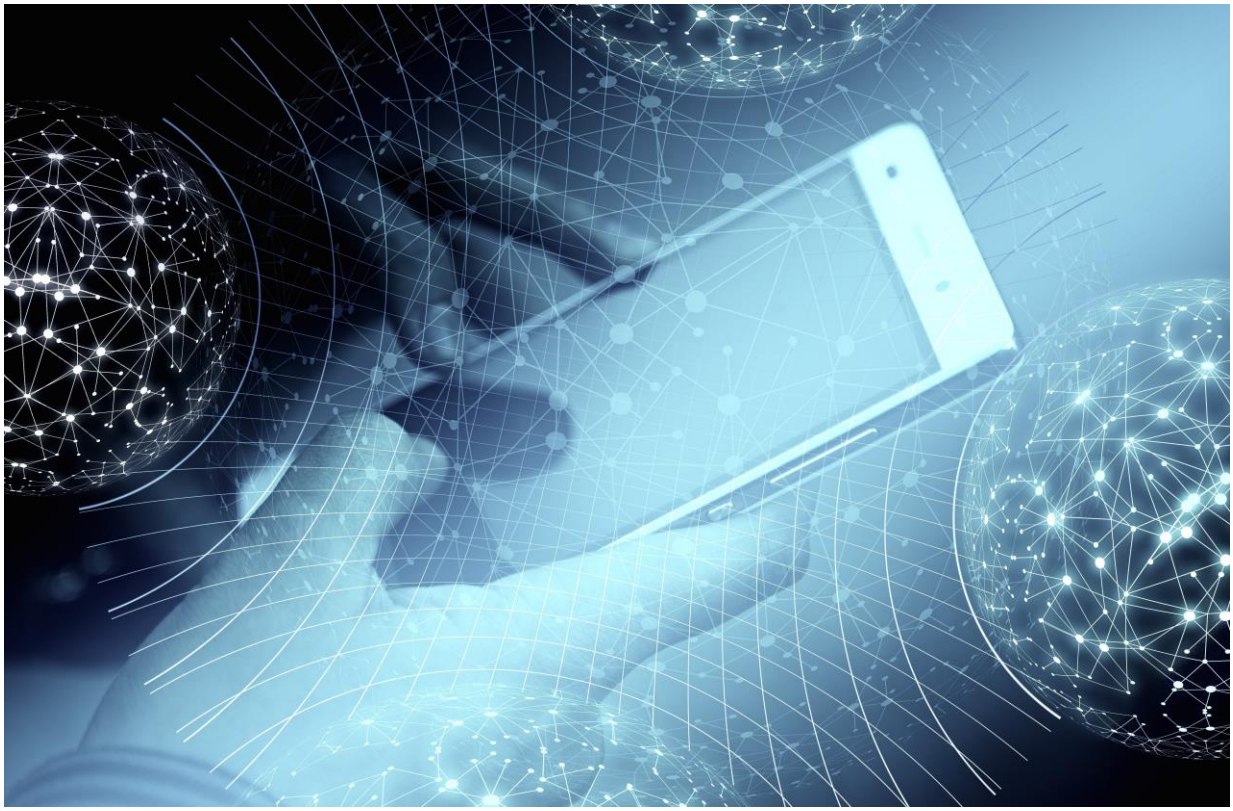
ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ СОЦИАЛЕН ФОНД

ОПЕРАТИВНА ПРОГРАМА ДОБРО УПРАВЛЕНИЕ

ДОКЛАД

ИЗСЛЕДВАНЕ НА ЕВРОПЕЙСКОТО ЗАКОНОДАТЕЛСТВО В СФЕРАТА НА КИБЕРСИГУРНОСТТА И ПРОУЧВАНЕ НА ДОБРИ И УСПЕШНИ ПРАКТИКИ ЗА КИБЕРЗАЩИТА НА ОБЩИНСКИТЕ АДМИНИСТРАЦИИ В ПРЕДОСТАВЯНИТЕ ОТ ТЯХ ЕЛЕКТРОННИ УСЛУГИ ЗА ГРАЖДАНИТЕ



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

Списък със съкращения **4**

I. Въведение **5**

II. Дефиниране на основните понятия **6**

1. Киберсигурност 6

2. Публичната администрация в контекста на киберсигурността 12

3. Критична инфраструктура 14

4. Киберпространство 15

5. Киберпрестъпност 17

6. Най-често срещаните видове киберпрестъпления 18

7. Електронните услуги в контекста на публичната администрация 22

8. Предизвикателства пред киберсигурността 24

III. Представяне на международния контекст. Европейско и национални законодателства в областта на киберсигурността **29**

1. Кое изискваше разработването на Директива МИС2? 33

2. Какъв е обхватът на МИС2 и кои са организациите предоставящи основни/критични услуги? 33

3. Какви са санкциите при неспазване на Директива МИС2? 35

4. Какви са основните цели и задачи на Директива МИС2? 35

5. Европейската агенция за киберсигурност (ENISA) 37

6. Преглед на 10 национални законодателства регулиращи политиките, приоритетите и мерките в областта на киберсигурността: Франция, Германия, Италия, Испания, Швеция, Нидерландия, Белгия, Полша, Естония, Румъния (+ България) 39

IV. Представяне на добри практики в сферата на киберсигурността на публичната администрация **57**

Естония 72

Германия 81

Франция 85

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

Италия 89

Испания 93

Нидерландия 96

Швеция 99

Белгия 101

Полша 103

Румъния 107

V. Изводи **111**

Използвани източници 118

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

Списък със съкращения	
ЕРИКС	Екип за реагиране при инциденти с компютърната сигурност
ЕС	Европейски съюз
ИКТ	Информационни и комуникационни технологии
ИТ	Информационни технологии
МИС2	Директива на ЕС за Мрежова и информационна сигурност
САЩ	Съединени американски щати
ФБР	Федерално бюро за разследване на САЩ
ANSSI	Национална агенция за киберсигурност на Франция
BSI	Федерална служба за информационна защита на Германия
CCN	Националнен криптологичен център на Испания
CERT-EE	Компютърен екип за спешно реагиране на Естония
CSU	Звено за киберсигурност на град Франкфурт
EDPB	Европейски съвет за защита на данните
ENISA	Европейска агенция за киберсигурност
EU-CyCLONe	Мрежа на ЕС за връзка при кибернетични кризи
EU-GDPR	Общ регламент за защита на данните на Европейския съюз
FASI	Агенция за сигурност на информационната система на Белгия
GCI	Глобален индекс на киберсигурността
IDPS	Система за откриване и предотвратяване на проникване в мрежата
IoT	Интернет на нещата
ITU	Международен съюз по телекомуникации
MFA	Многофакторно удостоверяване на идентичността
MSB	Агенция за непредвидени ситуации
NCC	Националният център за киберсигурност на Италия
NCSC-NL	Център за киберсигурност на Нидерландия
RIA	Агенция за информационна и системна сигурност на Естония
RRF	Механизъм на ЕС за възстановяване и устойчивост
VPN	Виртуална частна/защитена мрежа

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

Информационната сигурност има все по-нарастващо значение в стратегията на организациите за устойчивост и управление на рисковете. С напредъка на дигиталната трансформация, форсирана от глобалната пандемия Covid-19, въпросът за защитата на информационните и мрежови системи днес е особено валиден и за структурите на публичната власт. Това се изисква в контекста на електронните административни услуги, предоставяни от местната власт, както и заради съхраняването на чувствителна, поверителна информация за гражданите.

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.

Настоящият доклад цели да извърши пространствено изследване на предизвикателствата, които публичната администрация среща в сферата на киберсигурността. Защитата на мрежовата и информационна среда в контекста на електронните услуги, предоставяни от държавната администрация, е комплекс от технически и организационни мерки, които изискват отлично познаване на регулаторната рамка, както и планиране, приоритизиране, изпълнение и контрол над насоките, заложени в европейската и национална нормативна уредба.

Този доклад се стреми да изясни ролята, обвързаностите и произтичащите ангажименти на общинската администрация във връзка с новоприетата Директива за Мрежова и системна сигурност (МИС2) на Европейския съюз (ЕС), както и да разпише насоки и мерки в областта на превенцията срещу кибератаки.

Акцентът на доклада е върху изследването на нормативната база в областта на киберсигурността на европейско и национално ниво, както и на политиките и имплементирането на добри практики за превенция на киберпрестъпността в десет държави членки от Общността.

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

Киберсигурността се явява ключова политика и приоритетно направление в актуализираната стратегия на Европейския съюз за е-управление 2019 - 2025г. В тази връзка, за публичната администрация би било от полза да се запознае със спецификите на регулаторната уредба и да почерпи опит от успешните практики в превенцията на злонамерената дейност при електронните услуги. Това би способствало за изграждането на едно по-информирано разбиране на предизвикателствата в киберпространството и би спомогнало публичната администрация в отговорната задача да осигури ефективна дигитална сигурност на своите граждани.

Киберсигурността има транснационален характер и ефективната борба с киберпрестъпността може да бъде постигната единствено посредством цялостен (холистичен) подход, при който всички засегнати обекти и субекти действат при една унифицирана и равностойна нормативна, методологическа и техническа компетентност и подготовка. В тази връзка, усилията на българската държава и, респективно, публичната администрация, трябва да са насочени към това да достигнем средното за ЕС ниво на киберсигурност с цел пълноценна интеграция на българската държава и държавна администрация в европейските структури и политики за киберсигурност като доверен и силен партньор на техническо, оперативно и стратегическо нива.

II. Дефиниране на основните понятия

1. Киберсигурност

Възможността за пробив и компрометиране на дигиталното пространство, както и уязвимостта на електронните информационни масиви, винаги са били интегрална част от разбирането за същността на интернет мрежата, както и, респективно, за необходимостта от холистична стратегия за защитата на киберпространството и неговите потребители от недобросъвестни и зловредни действия.

Глобалната пандемия от Covid-19 и наложеното “затваряне” (“lockdown”) на обществено-социалния живот доведоха до безпрецедентен скок на хората, които разчитат на интернет за достъп до услуги и продукти, които

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

традиционно потребяват и получават в "реалния" живот, извън мрежата. В рамките на само няколко месеца човечеството се сблъска с предизвикателствата на една невиждана по мащабите и скоростта си дигитална трансформация на ежедневието, навиците и работния процес. Тази сеизмична промяна в начина, по който живеем и използваме интернет, доведе и до експонентното разпространение на киберпрестъпленията. Европейските държави отчетоха трицифрено увеличение, в процентно измерение, на докладваните инциденти с киберсигурността по време на пандемията (Европейска агенция за киберсигурност ENISA, 2022). Киберпрестъпниците адаптираха своите тактики, за да се насочат към хората в домовете им, които се превърнаха и в техни офиси. Работата от разстояние, в отдалеченост от защитата на мрежовите и информационни сървъри в офиса отвори "кутията на Пандора" за киберпрестъпниците да получат лесен достъп до чувствителни и поверителни данни, файлове, акаунти и пароли на стойност стотици милиарди долари. Хакерите атакуваха компютърната екосфера на потребители, компании, правителствени служби и цели глобални организации във време, когато киберзащитата бе хваната "в крачка" поради мащабите, скоростта и комплексността на предизвикателствата, с които трябваше да се справи.

Киберпрестъпниците използваха изпитани във времето тактики като "фишинг", "зловреден софтуер" ("ransomware") и "социално инженерство" (които ще разясним в детайли по-напред в доклада), за да въздействат на уязвимите потребители, изкарани извън защитената черупка на фирмената информационна и мрежова система**,** да предадат "доброволно" паролите и акаунтите си за достъп до фирмените тайни. Изследване на американския телекомуникационен гигант Verizon показва, че за компаниите средната цена за откупуване на откраднатa поверителна информация по време на пандемията е скочила до 22 000 долара на инцидент, спрямо 5000 долара преди глобалната здравна криза. Но цели 5% от успешните атаки са стрували на бизнеса 1 милион долара или повече, което е безпрецедентен процент успешни кибератаки в най-скъпия сегмент. Това е така, защото близо 85% от успешните пробиви на данни са включвали измама на служителите чрез фишинг и социално инженерство. Причините за това са в недостатъчната защитеност на домашните устройства и системи за работа, а също и в небрежността спрямо протоколите за сигурност от страна 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

служителите, както и в недостатъчната им осведоменост за рисковете и заплахите в киберпространството.

Историята на киберсигурността можем да проследим назад във времето, до зората на интернет. Започнала като един изследователски проект в университета Кеймбридж. Преподавателят по информационни технологии Робърт Томас създал програма, която да се "движи" свободно в интернет пространството, като оставя следа (съобщение) навсякъде, откъдето мине. Той нарекъл програмата си "пълзящо растение". Създателят на имейла, Реймънд Томлинсън, решил да доразработи идеята на своя колега, като направил така, че "пълзящото растение" да се възпроизвежда и дели всеки път, щом достигне определена компютърна мрежа или система. Паралелно с това Томлинсън създал втора програма, първообразът на антивирусния софтуер, която да преследва "вредителят" из Мрежата, за да го възпре и изтрие.

Преходът на компютърните компрометиращи вируси, от академичен експеримент до глобална престъпна мрежа и заплаха за свободните общества, следва изключително бързо и буйно развитие, обусловено от експонентно нарастващия достъп на хората до киберпространството и неговите ресурси. Интернет е неразривен аспект от съвременния свят, тъй като нашият личен и професионален живот все повече зависи от свързаните с него услуги и устройства. Това засяга ежедневието на все по-съществена част от световното население и има значително въздействие върху начина на живот и върху социално-икономическите взаимоотношения на държави и общества. Киберпространството предлага неограничени възможности за икономическо развитие, за социално включване и взаимодействие, както и поле за обмен на идеи и ресурси. Същото може да се каже и за целите на престъпните намерения в дигиталната среда.

Необходимостта от ефективна киберзащита придобива първостепенно значение за интернет потребителите, правителствата, публичната администрация и икономическите организации поради факта, че броят на кибератаките се е увеличил значително през последните години. Това бе допълнително форсирано от безпрецедентния процес на скоростна

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

дигитална трансформация на обществата, дошла в отговор на предизвикателствата, породени от глобалната пандемия Covid-19. Киберпрестъпността става все по-доходоносно занимание, за което свидетелства и годишният доклад на ФБР (Федерално бюро за разследване на САЩ) от 2021 година. В него глобалните финансови загуби от компютърни престъпления се оценяват на 4.2 млрд. долара. Това е със 700 милиона долара повече от предходната година, а в процентно измерение увеличението на жалбите за киберпрестъпления е 69%.

Тъй като все повече хора и организации стават част от интернет обмена, броят на потенциалните цели за кибератаки единствено ще се увеличава. В допълнение, сложността на тези атаки също се е подобрила, което прави по-трудно за хората и организациите да се защитят. Субекти от публичния и частен сектор предават чувствителни и поверителни данни през мрежи и към други устройства в хода на извършване на дейност, а киберсигурността описва дисциплината, посветена на защитата на тази информация, и системите, използвани за нейната обработка или съхранение. Тъй като обемът и сложността на кибератаките нарастват, компаниите и организациите, особено тези, на които е възложено да защитават информация, свързана с националната сигурност, здравето или финансовите записи, трябва да предприемат изпреварващи стъпки за защита на своята чувствителна информация. Тази непрестанна и неравна “гонитба” срещу иновативността и все по-голямата комплексност на онлайн измамите се явява и най-голямото предизвикателство за киберсигурността.

Статистическата възможност през 2023 година човек да стане жертва на зловредна практика в интернет също се е увеличила многократно на фона на подобни изследвания, правени през 2011 година. Последствията от такава атака също единствено нарастват в своята сериозност. Те могат да доведат до чувствителни финансови загуби; увреждане на репутация и загуба на поверителна информация; забавяне и дори пълно “разграждане” и спиране на оперативния процес в организациите; увреждане и кражба на база данни, което може да има сериозни последици както за отделни лица, така и за цели отрасли на индустрията.

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

За важността на киберсигурността в контекста на днешните предизвикателства говори и фактът, че в стратегическите харти, както на Европейският съюз, така и на Съединените американски щати (САЩ), още от 2013 години кибератаките и дигиталното шпиониране са определени за основна заплаха за националната сигурност, засенчвайки в някои сфери и аспекти дори тероризма. В този доклад ще разгледаме в детайли и най-новата, преработена стратегия на Европейския съюз в областта на киберсигурността. Целта на тази стратегия е да се засили устойчивостта на Европа срещу киберзаплахи и да се гарантира, че всички граждани и предприятия могат да се възползват в пълна степен от надеждни услуги и цифрови инструменти. Новата стратегия съдържа конкретни предложения за въвеждане на регулаторни, инвестиционни и политически инструменти, като в своята преработена версия съдържа и препоръки за публичната администрация.

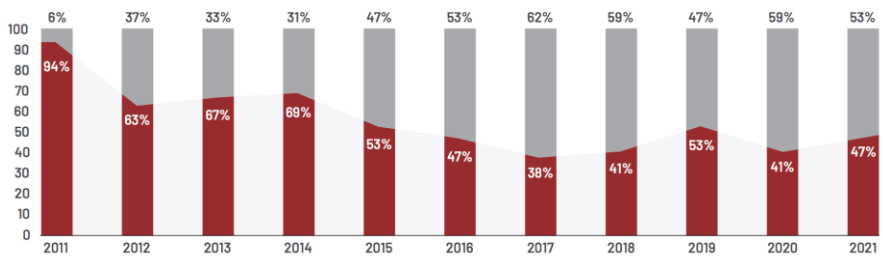
Киберсигурността, в по-широк контекст, може да се дефинира като набор от технологии, методи и процеси, предназначени да защитават от неоторизиран достъп, атака или повреда електронните мрежи, компютърните и мобилни устройства, сървърите, операционните системи и програми, както и информационните база данни. В същността си киберсигурността е нормативната и технологична защитна “стена” на информационните технологии. Дефинира се още и като защита и запазване на конфиденциалността, целостта и достъпността на информацията. Процесът по осигуряване не защита в дигиталното пространство изисква много повече от обикновен технически метод и контрол, а се нуждае от човешки ориентиран подход в изграждането на култура на киберсигурност. Това е от първостепенно значение, защото помага за защита на лица и организации от пробиви на данни, кражба на самоличност и други форми на киберпрестъпления, които могат да причинят значителни материални, нематериални вреди и правни последствия. Също така защитата на базата данни е важно условие за поддържане на доверието в дигиталната мрежа и за гарантиране, че чувствителната информация, като например финансови данни, интелектуална собственост, патенти, идентификационни данни за вход и друга лична информация, остава поверителна и неприкосновена.

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

Киберзащитата може условно да се раздели на два подвида – такава, осигурена от външен или от вътрешен източник. Външен източник на киберзащита са правителствени агенции или организации, които разкриват и предупреждават частни фирми и компании за възможно компрометиране на техни данни или системи. Вътрешен източник на киберзащита пък са ИТ отдели в самите частни организации. Това е важно уточнение, защото характеризира дългия път, който компаниите са извървели в разбирането, че превенцията на престъпленията в дигиталното пространство е обща кауза, в която трябва да си партнират всички участници, както и онагледява стратегическата важност, която инвестициите в информационна и дигитална защита заемат в живота на организациите.

Долната графика разглежда периода между 2011 и 2021 година и показва компрометирането на глобалните информационни системи по източник на разкриване на киберпрестъплението. Резултатите показват, че за 10-годишен период от време организациите са инвестирали и обучили собствени, вътрешни, екипи по киберсигурност, които са намалили от 94% на 47% зависимостта си от външни източници на защита. Иначе казано, през 2021 година организациите са разчитали в повече от половината случаи на разкритие на компрометиране на мрежи, данни и системи на собствените си ИТ отдели. Това е важен успех в стратегията киберсигурността да се превърне в устойчива, всеобща кауза, в която публичния и частен ресурс да си сътруничат в обмена на информация и успешни практики.

Компрометиране на глобалните информационни системи за периода 2011 – 2021 по източник на разкриване на киберпрестъплението



- външен източник - вътрешен източник

* Данните са от годишния доклад на компанията за киберсигурност Mandiant (дъщерно дружество на Google)

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

2. Публичната администрация в контекста на киберсигурността

Съвременният модел на публичната администрация е формиран в съвкупност от комплексни политически, социални и икономически фактори. Административните функции в обществен интерес се изпълняват въз основа на законови разпоредби при условията на прилагане на специфични правила за вземане на решения, както и техники за организация на работния процес, които включват принципи и процедури при изпълнението на оперативните и технически задачи.

В контекста на киберпространството гореспоменатите характеристики определят публичната администрация като сбор от операции, изпълняващи се в мрежовата и информационна среда. Трансформациите, свързани с компютъризацията на работния процес и обслужването на гражданите, както и повсеместното разпространение на информационни и комуникационни технологии, означават, че задължението на публичната администрация в днешната информационна ера е, от една страна, да синхронизира дейностите и услугите по обслужване на гражданите, а от друга, да управлява сложни информационни мрежи и системи. В допълнение, публичната администрация има задължението постоянно да се адаптира, на нормативно и оперативно ниво, към функционирането и използването на нови технологии, като взима предвид всички рискове и заплахи, които произтичат от това.

За структурите на местната власт информационната и мрежова сигурност е сравнително ново понятие. Автоматизираната обработка на данни и информация днес играят все по-ключова роля при изпълнението на функциите на администрацията. Всички основни процеси вече са поддържани от информационните и комуникационни технологии (ИКТ). 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.

Повишеното използване на съвременните ИКТ значително увеличи риска информационната инфраструктура да бъде компрометирана и засегната както от умишлени и злонамерени външни атаки, така и от действия 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

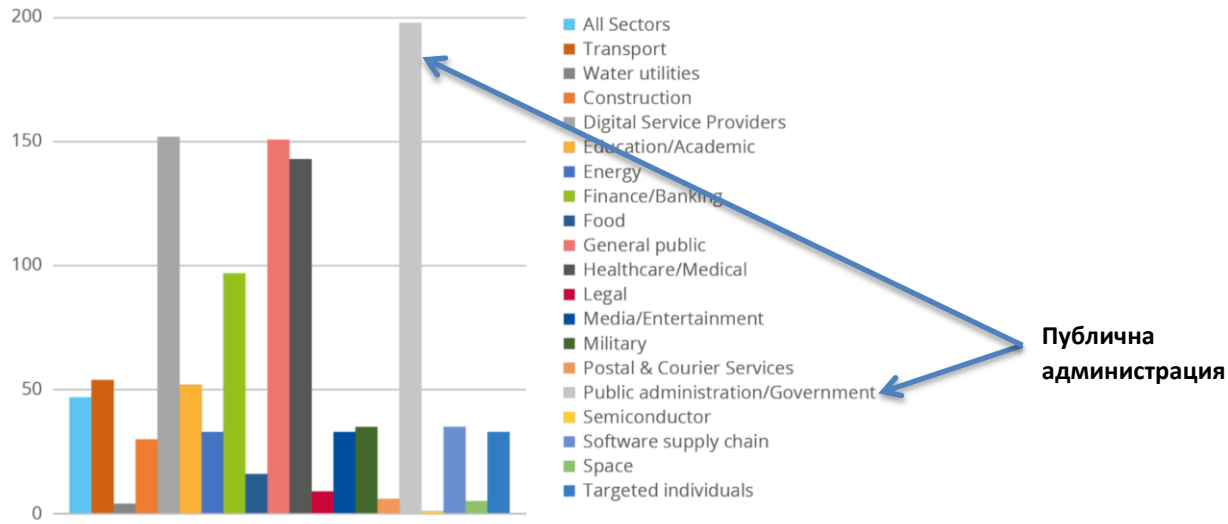
служители, дали от небрежност и немарливост към протоколите по сигурността, или поради недостатъчна степен на осведоменост и знание за рисковете в киберпространството. Именно човешкият фактор е водещият риск за всяка една общинска структура в сферата на киберсигурността. Изследване от 2021 година сред малките и средни общини във Франция, дело на Института за киберсигурност, показва високият процент дивиация и неравномерност в разбирането и информираността за рисковете в киберпространството спрямо по-големите общини. В по-малките общини проблемът все още се възприема като чисто технически, който трябва да включва единствено определени лица със специализирани умения. При по-малките общини въпросите на киберсигурността все още се подценяват и при тях липсва разбирането за необходимостта от интегриран подход с междуфункционална визия за решаване на проблемите, както и инвестиране в обучение и повишаване компетентността и осведомеността на служителите.

Липсата на стандарт за информационна и мрежова защита може да доведе до чувствителни смущения в изпълнението на задачите на публичната администрация, което може да намали ефективността на органите и в крайни случаи да доведе до спиране на техните процеси. На този фон осигуряването на информационна сигурност е една от централните задачи на местните власти, в рамките на която трябва да се организира 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 базата данни могат да доведат до блокиране на обществени услуги, кражба на чувствителни данни, което се явява и заплаха за националната сигурност на всяка една страна.

Изследване на Европейската агенция по киберсигурност (ENISA) по време на “най-горещата” част от пандемията Covid-19 показва, че най-атакуваната от киберпрестъпници сфера на обществено-социалния живот в държавите от ЕС е била именно публичната администрация/правителствените учреждения. За това свидетелства и долната графика.

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

Брой докладвани пробиви в системата за сигурност в ЕС за периода април 2010 – май 2021 година, по отрасъл



* Данните са от годишния доклад на Европейската агенция по киберсигурност (ENISA)

3. Критична инфраструктура

Съвременният живот все повече зависи от широк набор от функции, услуги, системи и активи, обикновено наричани с термина инфраструктура. Днес правителствата разглеждат някои от разновидностите на тази взаимносвързана екосистема като, например, комуникациите, банкирането, енергетиката, транспорт, комунални услуги, здравеопазване, публична администрация, за критично важни. Причината за това е, че всяко прекъсване, компрометиране или унищожаване на елементи от тази взаимносвързана екосистема може да повлияе драстично на стабилността и функционирането на цялата национална, икономическа, политическа и социална система за сигурност (Майкрософт, 2020). В този смисъл, защитата на критичната инфраструктура от нарастващия брой и комплексност на кибератаките е от първостепенно значение за всяка една държава и е залегнало в стратегическите усилия и регулаторни наредби за борба с киберпрестъпността.

Директива 2008/114/ЕО на Съвета на ЕС от 8 декември 2008 г. относно идентифицирането и обозначаването на европейската критична инфраструктура и оценката на необходимостта от подобряване на тяхната защита представлява важен документ в това отношение. По-специално,

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

тази директива на Европейския съюз определя критичната инфраструктура като „актив, система или част от нея, разположени в държави членки, които са от съществено значение за поддържането на жизненоважни обществени функции, здраве, безопасност, сигурност, икономическо или социално благосъстояние на хората и чието прекъсване или унищожаване би имало значително въздействие в държава членка в резултат на невъзможността да се поддържат тези функции“. Публичната администрация, заради характера на своята дейност и услуги и заради информацията, която съхранява и с която борави, е част от дефиницията за критична инфраструктура.

4. Киберпространство

Терминът често се използва взаимозаменяемо с понятието “интернет”. Можем да приемем, условно, че киберпространството представлява цялата област от информационни ресурси, налична чрез компютърните мрежи. В технологичен смисъл то включва всички елементи на електронните мрежи, софтуерните и хардуерни продукти, както и съществуващите бази данни и информационни масиви. По своята същност киберпространството е средата, в която всички обекти на изследването в областта на киберсигурността (киберпрестъпност, кибервойна, кибертероризъм, киберсигурност) възникват и оперират. Следователно политиките в областта на киберсигурността целят защитата на киберпространството.

То се отличава като интерактивна, комуникационна среда, чрез която всеки, който има достъп до нея, може свободно да разпространява и получава единици информация. В киберпространството липсват национални граници и трансгранични законодателни разпоредби, което при съвременните възможности на технологиите улеснява достъпа както на легитимни субекти, така и на лица, групи и институции с криминални намерения да оперират. Това прави киберпространството особено уязвимо и податливо на широк спектър от нерегламентирани дейности. За ефективна киберсигурност една публична администрация или бизнес организация трябва да координира усилията си в цялата си информационна система.

Елементите на кибернетичното пространство включват:

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

1.Мрежова сигурност: Процесът на защита на мрежата от нежелани потребители, атаки и проникванията.

2.Сигурност на приложенията: Приложенията изискват постоянни актуализации и тестване, за да се гарантира, че тези програми са защитени от атаки (например, използването на антивирусни програми).

3.Сигурност на крайната точка: Отдалеченият достъп е необходима част от работния процес, но може да бъде и слабо място за данните. Сигурността на крайната точка е процесът на защита на отдалечения достъп до мрежата на компанията.

4.Сигурност на данните: Данните са вътре в мрежите и приложенията. Защитата на поверителната информация за гражданите е отделен слой на сигурност.

5.Управление на идентичността: По същество това е процес на разбиране на достъпа, който всеки индивид има в организацията.

6.Сигурност на база данни и инфраструктура: Всичко в една мрежа включва бази данни и физическо оборудване. Защитата на тези устройства е от първостепенно значение.

7.Сигурност в облака: Много файлове са в цифрови среди или „облака“. Защитата на данните в 100% онлайн среда идва с голям брой предизвикателства.

8.Сигурност за мобилните устройства: Мобилните телефони и таблети включват практически всеки тип предизвикателство за сигурността сами по себе си.

9.Възстановяване след бедствие и планиране на непрекъснатост на операциите: В случай на пробив в сигурността, природни бедствия или други форсмажорни събития, данните трябва да бъдат защитени, за да може дейността да продължи. За целта е необходим кризисен план за действие, с ясно начертани роли, стъпки, отговорности и срокове.

10.Обучение на крайния потребител: Потребителите може да са служители, които имат достъп до мрежата, или клиенти, влизащи чрез приложение. Възпитаването на добри навици (смяна на парола и наличие на силна

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

парола, двуфакторно удостоверяване и т.н.) е важна част от защитата на кибернетичното пространство и способства повишаване компетентността и културата на потребители и служители в сферата на киберсигурността.

5. Киберпрестъпност

Киберпрестъпността може да се дефинира като „Незаконно използване на всяко комуникационно устройство за извършване или улесняване на извършването на каквото и да е незаконно действие“ (Майкрософт, 2021). То е вид престъпление, което се опосредства чрез използването на компютърна система и устройство и е насочено към компрометирането на друга компютърна система и устройство. Може да бъде индивидуално или екипно и да бъде насочено както към отделни лица, така и към бизнес групи, частни и публични организации, правителства и др. Голяма част от кибератаките срещу информацинните системи и данните, съхранявани в тях, са престъпления с цел финансови облаги. Други са свързани с рекет, изнудване, кражба и нарушаване на правата на интелектуалната собственост, шпионаж, а в днешните условия виждаме, че и в контекста на военни конфликти, киберпрестъпления, поощрявани и спонсорирани от правителства, са насочени към обекти от критичната инфраструктура на дадена държава за постигане на военни цели.

За киберпрестъпник е прието в по-широк и разговорен контекст да употребяваме термина “хакер”. За такъв се приема субект, притежаващ умението да проникне без разрешение в компютърните мрежи и системи на чужд субект или организация, с цел извличане на полза. Важно е да се отбележи, че не всеки “хакер” се класифицира автоматично като киберпрестъпник. Определящият фактор дали е такъв е мотивът на деянието, който не трябва да се приема по подразбиране като задължително злонамерен.

Хакери - Така нареченото “хакване” е процес по разкриване на определена уязвимост в мрежа или система. Субекти или група от субекти, чиито действия не са насочени към нанасянето на вреда, а са ангажирани в използването на компютърните си умения за разкриване на пробиви и слабости в компютърните мрежи и системи, се наричат **“white hat” (бели шапки).** Подобни хакери подпомагат дейността на официалните служби, 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

да бъдат слабостите в системите навременно отстранени и да се подобри защитата на информационното пространство.

От друга страна, "хакването" се счита за киберпрестъпление, когато има злонамерена цел за извършване на незаконни, деструктивни дейности като измама, кражба, рекет, изнудване, пиратство срещу чужда собственост и субект или група субекти без тяхното знание и съгласие. Това са така наречените **"black hat" (черни шапки).** Наричат се още "кракери".

Киберпрестъпниците непрекъснато еволюират в способите и техниките за компрометиране и кражба на поверителна информация, така че откриването и предотвратяването на този тип заплахи става все по-предизвикателно. Нещо повече, с тенденцията за дистанционна работа и предоставянето на привилегирован достъп на отдалечени от защитената работна мрежа служители, единствено усложнява работата на ИТ отделите (отдел "Информационни технологии") по осигуряванто на ефективна защита на мрежите и системите.

Очаква се глобалните щети от киберпрестъпления да струват на световната икономика общо 10,5 трилиона долара до 2025 г. (Cybersecurity Ventures). Президентът на европейския отдел за киберсигурност пък докладва, че през 2021 година, в рамките на ЕС, е имало повече сигнали за компрометирани данни и системи, отколкото през която и да е било друга година от 2003 насам, когато е започнало да се събират данни.

6. Най-често срещаните видове киберпрестъпления

1. Фишинг измама:

Това е най-разпространеният вид кибератака, като на дневна база в глобалната мрежа се разпращат стотици милиони имейли с подобно съдържание. Подателите на **фишинг** съобщенията се представят за легитимни източници и целят да придобият от "жертвата" конфиденциални данни, свързани с номера на сметки, местоживеене, месторабота и пароли. Фишингът е вид атака чрез социално инженерство. Типичен пример за подобна схема са имейлите, в които ви съобщават, че сте спечелили от лотария, бинго, "Зелена карта", или пък нигерийски принц иска да сподели с вас многомилионното си наследство и ви кани да

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

предоставите личните си данни и банкови сметки, по които да ви бъдат преведени средствата.

Потребителите трябва да бъдат също изключително мнителни за имейли, които имитират тези на банки, мобилни оператори, комунални услуги, които подканват да натиснете на определен линк, където да смените паролата си или да предоставите данни. Друга разновидност на фишинг измамите са **фарминг** имейлите, които пренасочват автоматично "жертвата" към нов, "кух" сайт, без тя да разбере. Така под претекст и с вяра, че попълва данни и пароли в легитимния сайт на своята обслужваща банка, например, получателят на фарминг имейла всъщност предоставя поверителната си информация на киберпрестъпниците.

2. Зловреден софтуер (Ransomware атака):

Атаките със зловреден софтуер са много често срещан вид киберпрестъпления. Този компютърен вирус има способността да попречи на потребителите да получат достъп до своите пароли и лични данни в системата, като ги криптира. За да възстановят достъпа до системите и мрежите киберпрестъпниците изискват откуп. Едни от най-крупните случаи на измами в света са именно с рансъм вирус.

Най-голямата подобна атака, за която е публично известно, се случва през май 2021 година, когато системите на американската петролна компания Колониъл Пайплайн (Colonial Pipeline) са "отвлечени" от хакери. Компанията, която осигурява повече от половината петролни доставки за Източния бряг на Съединените Щати, е блокирана в цялата си дейност. Повече от 10 000 бензиностанции са оставени без гориво. По информация, потвърдена публично от изпълнителния директор на компанията, Колониъл Пайплайн е заплатила откуп в размер на 3,5 милиарда долара, за да получи обратно достъпа до своите кодове за декриптиране на паролите и информацията и да възобнови дейността си.

3. DdoS атака:

Атаките DdoS (Distributed denial-of-Service) имат за задача да блокират и предотвратят достъпа на потребителите до критична информация или до определени сайтове. Този вид вируси са ефективни и лесни за изпълнение и управление, затова намират и широко приложение. DdoS атакуват

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

мрежовите системи, като използват предварително подготвена "армия" от ботове (фалшиви профили с определена, целенасочена задача), които заливат "жертвата" с трафик или информация, докато не сринат услугата/сайта и те не станат недостъпни. Атаката с DdoS действа по два начина: а/ изчерпва пропусквателната способност на сайта/канала за връзка с интернет; б/ изчерпва изчислителните способности на сървъра (памет, процесорно време, дисково пространство).

Публичната администрация, както и сайтове, асоциирани с правителствени организации и партии, са честа "жертва" на подобни атака.

4. Кражба на самоличност:

Кражба на самоличност възниква, когато киберпрестъпник използва лични данни на друго лице като номера на кредитни карти или лични снимки, без тяхното разрешение, за да извърши измама или престъпление. Типичен пример е използването на данни от банкови карти за покупката на стоки или услуги в интернет от името на лицето, чиито данни са откраднати. Целта е финансова изгода.

5. Хакване/злоупотреба с компютърни мрежи:

Този термин се отнася до престъпление, свързано с неоторизиран достъп до частни компютри или мрежи и злоупотреба с тях или чрез кражба на данни и информация, или чрез изключване, изтриване, подправяне на съхранените данни, както и други незаконни подходи, с които се цели информационна или финансова кражба.

6. Кибертормоз, изнудване, преследване и измами в социалните мрежи:

Известно е още като онлайн или интернет тормоз. Включва източване на лична информация, видео, снимки от устройството или мрежата на жертвата с цел изнудване. Обикновено киберпрестъпникът заплашва, че ще разпрати или сподели публично лично съдържание, което може да унизи и уязви жертвата, ако същата не направи паричен превод, за да го "откупи". Напоследък този тип киберпрестъпление става много разпространено, особено сред тийнейджърите.

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

Киберизнудването е искане на пари от киберпрестъпниците, за да върнат някои важни данни, които са откраднали, или да спрат да извършват злонамерени дейности, като атаки за отказ на услуга.

Киберпреследването може да се определи като получаване на постоянно и нежелано съдържание от някого, като телефонни обаждания, съобщения, заплахи, провокативни и обидни послания, снимки, видео, с цел контролиране и сплашване.

Използването на фалшиви акаунти в социалните медии е много често разпространен начин за извършване на всякакъв вид зловредни или дезинформационни дейности, като представяне за други потребители или изпращане на сплашващи или унизителни съобщения, както и разпространяването на фалшиви новини с цел икономическа или политическа изгода.

7. Софтуерно пиратство и нарушение на интелектуална собственост:

Софтуерното пиратство е незаконно използване или копиране на платен софтуер с нарушаване на авторски права или лицензионни ограничения. Пример за софтуерно пиратство е, когато изтеглите ново неактивирано копие на Windows и използвате това, което е известно като „Кракове“, за да получите валиден лиценз за активиране на Windows. Това се счита за софтуерно пиратство и кражба на интелектуална собственост. Същото се отнася за музика, филми, снимки, промишлени дизайни, изкуство и прочие.

8. Онлайн трафик на оръжия и наркотици посредством криптовалути:

С големия възход на технологията за криптовалута се опосредства прехвърлянето на парична стойност или еквивалент по сигурен и криптиран начин. По този начин все по-често се извършват сделки с наркотици, без да се привлича вниманието на правоприлагащите органи или същите да имат механизъм да проследяват подобни сделки. Това доведе до нарастване на предлагането и закупуването на лекарства, оръжия и наркотици в интернет чрез “тъмната мрежа”.

Данни на европейската компания за киберзащита Ekran за 2021 година показват, че за публичната администрация “зловредният софтуер” (ransomware) е бил на първо място в докладването на инциденти 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

търсенето на помощ, като увеличението спрямо 2020г. е с 5%. На второ място се е изкачил "фишингът", като при него увеличението на инцидентите за местната власт е от впечатляващите 60%. Хакването на онлайн акаунти и кражбата на пароли запазва трето място, с 50% ръст спрямо предходната година. Що се отнася до нарушенията на сигурността на личните данни, те се покачват през 2021 г. от девето на четвърто място, с +75%.

7. Електронните услуги в контекста на публичната администрация

Електронното правителство, в най-общ план, представлява дигитализация на процедурите, документите и административните услуги с цел подобряване, улесняване и хармонизиране на управлението и обслужването на гражданите и бизнеса чрез използването на съвременни технологии в сферата на мрежовите и информационни системи (ENISA, 2021).

Примери за електронни услуги, които електронното правителство на общинско ниво може да предоставя на гражданите си са: онлайн плащане на местни налози, такси и сметки (например, данък върху собствеността или сметки за комунални услуги); подаването на онлайн заявления, посредством електронен подпис (например, разрешение за строеж); достъп до публична или лична информация като протоколи от заседания на общински съвети, бюджет, кадастър, данъчни оценки, история на собственост и наследственост; онлайн заявка за обществени услуги като сметосъбиране, поддръжка на улици, извозване на обемисти предмети или опасни отпадъци; онлайн регистрация на избиратели и изборна информация, включително и гласуване по интернет; онлайн кандидатстване за субсидии и помощи; онлайн заявка за ремонт на публична инфраструктура (например, улично осветление, пътна сигнализация); онлайн докладване на нарушения като неправилно паркиране, нарушения на кодекса на труда или опасности за околната среда; онлайн обяви за работа и подаване на кандидатури и др.

Насърчаването на дигиталната трансформация на държавната и местна власт остава основен приоритет за Европейския съюз. В преследване на амбицията "Цифрово десетилетие на ЕС", Европа има за цел да предоставя

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

всички ключови обществени услуги онлайн до 2030 г. В подкрепа на стратегията държавите членки гласуваха да разпределят повече от 26 % от общите разходи по Механизма на ЕС за възстановяване и устойчивост (RRF) именно за дигиталния преход. Коронавирусът (Covid-19) постави на изпитание гражданите, бизнеса и правителствата. Това накара Европа да преосмисли стойността и значението на цифровизацията и начина, по който се предоставят публичните услуги. Доклад на Европейската комисия за усилията на държавите членки през 2020 и 2021 година да трансформират своята публична администрация в електронно правителство, изследва степента на зрялост, достигната от държавите в процеса на дигитализация. Зрелостта се измерва в следните четири компонента:

1.Ориентираност към потребителя: До каква степен услугите се предоставят онлайн? Доколко са удобни за мобилни устройства? Какви механизми за поддръжка, защита от киберзаплахи и обратна връзка съществуват?

2.Прозрачност: Публичните администрации предоставят ли на гражданите си ясна информация за това как се предлагат техните услуги? Прозрачни ли са по отношение на процесите по изготвяне на политики за осигуряване на електронни услуги, както и относно начина, по който се обработват личните данни на гражданите?

3.Ключови фактори: Какви технологични фактори са налице за предоставяне на услуги на електронното правителство? Как се оценява тяхната комплексност и защитеност?

4.Трансгранични услуги: Колко достъпно и лесно е за гражданите от чужбина да използват онлайн услугите на публичната администрация? Какви механизми за поддръжка, защита от киберзаплахи и обратна връзка съществуват?

Въз основа на горепосочените измерватели, към които в анкетните карти на всяка държава са получени отговори по 48 уточняващи въпроса, страните членки са сформирали общ резултат за зрялост на електронното си правителство. Този резултат варира от 0% до 100% и е показан на графиката по-долу.

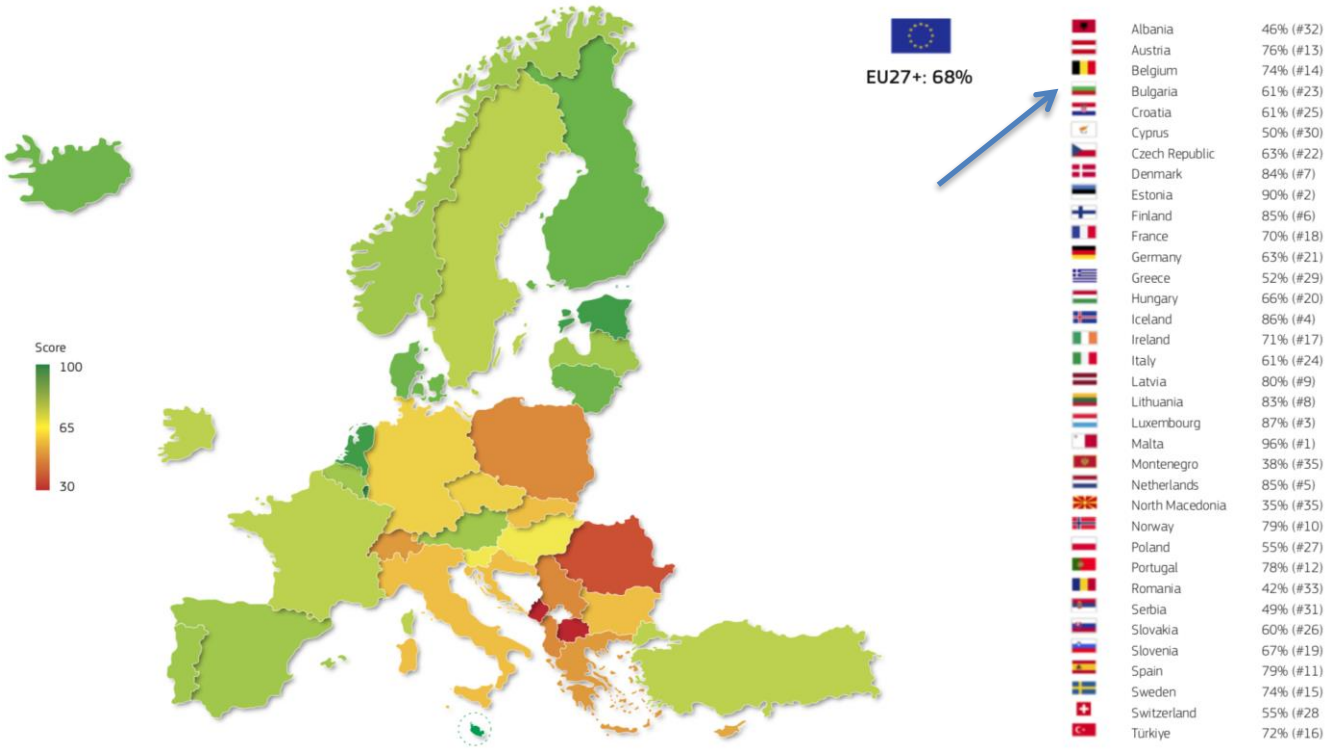
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление“ 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

Европейските лидери в областта на електронните услуги са Малта (96%) и Естония (90%). Техните електронни правителства се оказват най-ориентирани към потребителите, най-прозрачни, технологично развити и защитени, както и отворени за потребители от други европейски страни.

Като лидери се открояват също Люксембург (87%), Исландия (86%), Нидерландия (85%), Финландия (85%), Дания (84%), Литва (83%), Латвия (80%), Норвегия (79%), Испания (79%) и Португалия (78%).

Общото представяне в ЕС27 + трети страни е средно 68%.

България е класирана на 23-то място с резултат от 61%, който е под средното равнище за ЕС27+. Резултатите от изследването са показани на графиката по-долу.



*Европейска комисия, 2022

8. Предизвикателства пред киберсигурността:

Предизвикателствата за справяне с киберпрестъпленията, пред които са изправени организациите от частния и публичния сектор, както и гражданското общество, са значителни. Те изискват взаимодействие и унифициран отговор от всички участници в киберпространството, тъй като една от многото специфични характеристики на киберпрестъпността е

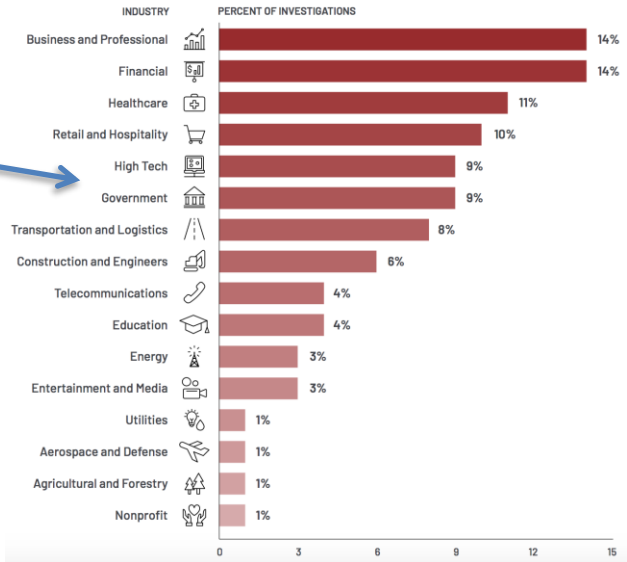
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни", финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление" 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

нейният наднационален характер. Нито една организация или институция, била тя частна или държавна, не може да се справи самостоятелно с предизвикателствата и рисковете на киберсигурността. Това обуславя създаването и поддържането на ефективна трансгранична нормативна база, която да спомага борбата с този вид престъпления. Само енергичните действия в тази посока ще насърчат сигурно, стабилно и отворено киберпространство. Освен това правните и политическите рамки ще трябва да се адаптират за по-добро зачитане и прилагане на международните норми за правата на човека, като същевременно се борят ефективно с киберпрестъпността, злонамерените кибердействия, кибератаките, както и използването на интернет за терористични цели и насърчаването на насилствен екстремизъм.

Долната графика, която показва процентното измерение на киберпрестъпленията в глобален план за 2021 година, ни дава показателна представа за това колко разнородна е структурата на киберпрестъпността спрямо отраслите на обществено-икономическата дейност. С други думи, киберпрестъпниците разполагат с ресурсите, уменията и интереса да атакуват всяка една сфера на обществото, икономиката и политиката. Това показва, че ролята и необходимостта от ангажираност на всички субекти и обекти с досег до киберпространството, за управление на рисковете и заплахите от кибератаки, е голяма.

Таргетиране от киберпрестъпниците на обществените сфери, 2021

Публична администраци



* Данните са от годишния доклад на компанията за киберсигурност Mandiant (дъщерно дружество на Google)

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

Кои са основните предизвикателства в сферата на киберсигурността, пред които е изправена публичната администрация?

1. Липса на опит в областта на киберсигурността: Много общински власти, особено по-малките, не разполагат с ресурси или опит, за да защитят адекватно своите системи и мрежи от кибератаки.

2. Постоянна еволюция на заплахите: Киберпрестъпниците непрекъснато разработват нови тактики и техники за избягване на системи за откриване на софтуер, пригоден за компрометиране. Това означава, че общинските власти трябва постоянно да инвестират в обучение и да актуализират своите мерки за киберсигурност, за да изпреварят тези заплахи.

3.Комплексната ИТ среда: Съвременните административни власти разчитат на разнородни технологии и системи, за да извършват своите операции, което затруднява защитата на всяка потенциална уязвимост.

4. Ограничени бюджети: Киберсигурността може да бъде скъпо начинание и много общински власти, особено по-малките, може да нямат ресурсите да инвестират в стабилни мерки за киберсигурност.

5. Човешка грешка: Въпреки най-добрите усилия, кибератаките все още могат да бъдат успешни поради човешка грешка, като, например, служители да станат жертва на фишинг атаки или при неспазване на правилните протоколи за сигурност.

Най-значимото предизвикателство в сферата на киберсигурността е непрекъснато и агресивно развиващият се характер на самите рискове. Традиционно организациите от частния и публичния сектор са фокусирали по-голямата част от своите ресурси върху сигурността на периметъра или иначе казано, за да защитят своите най-важни системни компоненти срещу ограничен брой най-разпространени и известни заплахи. Днес този подход е недостатъчен, тъй като рисковете се увеличават и променят по-бързо, отколкото организациите могат да се справят. В резултат на това ИТ експерите насърчават по-проактивни и адаптивни подходи към киберсигурността, като преминаване към непрекъснато наблюдение и оценки в реално време и подход към сигурността, фокусиран върху данните, за разлика от традиционния модел, базиран на периметъра.

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

Значението на този нов подход в контекста на сигурността както на хората, така и на държавите, нарастна неимуверно, тъй като технологиите продължават да се развиват и напредват, давайки тласък на компютъризацията във всичките ѝ форми и широко разпространения достъп до Интернет. Този директен достъп до информация, наличен благодарение на бързото развитие на компютърните системи, сега е един от основните определящи фактори за социалния и икономически растеж и често определя успеха или провала на едно начинание.

Достъпът до мрежови услуги може да бъде инструмент за насърчаване или контролиране на специфични поведенчески модели като, например, политически решения. Действията, предприети от различни участници в киберпространството, могат да доведат до конкретни икономически, социални или политически резултати. Това превръща киберпространството в област, която засяга сигурността на публичния и частния сектор и на обществата като цяло.

Прилагането на технически методи като единствено и достатъчно решение на проблема с киберсигурността е слабоефективно и доказало се като недостатъчно условие за защита от зловредни дейности в киберпространството. За организациите и администрацията е от критично значение да култивират и поддържат култура на познаване и бдителност спрямо киберпрестъпленията.

Служителите трябва да бъдат активно и редовно обучавани за рисковете и заплахите на киберпространството, включително как да се защитят. Успешна практика е служителите да получат поведенческа подготовка и да бъдат стимулирани да я практикуват в ежедневната си работа. Мнозинството експерти в областта на киберсигурността се обединяват около твърдението, че най-добрата защита за компаниите и администрацията е обучението на служителите в разпознаването на киберзаплахите. Инвестирането в продукти за информационна сигурност не може да гарантира пълна защита, ако не бъде придружено от програми за обучение и сертификация. Намаляването на риска от човешка грешка е ключът към по-добрата превенция, но също и едно от големите предизвикателства, с които трябва да се справят структурите на местната 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

В какви приоритетни направления трябва да бъдат насочени усилията за ефективна киберсигурност от стратегическа, холистична гледна точка?

1. В изграждане на национална екосистема за киберсигурност чрез фокусиране върху функционалността и ролята на националните и секторни Екипи за Реагиране при Инциденти с Компютърната Сигурност (ЕРИКС). Укрепване на капацитета и развитие на възможностите на националните ЕРИКС за наблюдение на националното киберпространство, откриване на уязвимости, предотвратяване и реагиране на кибер инциденти и кризи от различен мащаб, както и постигане на пълна интеграция на България в европейската екосистема за киберсигурност;

2. Внедряване на платформа за сътрудничество и инструменти за партньорство за споделяне на информация в областта на киберсигурността;

3. Имплементиране на принципите на киберетиката между партньорите и в процесите на обмен на информация, чрез разработване и налагане на Етичен кодекс за киберсигурност;

4. В изграждане на сигурна среда за киберсигурност за уязвимите публични и частни институции, чрез предоставяне на ресурси, съвети и услуги за централизиран мониторинг и защита;

5. В изграждане на интегрирана система за киберотбрана за защита на споделените информационни ресурси на електронното управление;

6. В разработване на система и методология за анализ на изходния код за откриване и коригиране на уязвимости и грешки на приложенията, при внедряване, надграждане или разработване на информационна система.

7. В инвестиране в осведомителни кампании и обучения за служители и потребители, чрез които те да бъдат запознати с рисковете и заплахите за сигурността в киберпространството, както и да получат практически насоки и наставления за това как да се справят с въпросните заплахи.

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

III. Представяне на международния контекст. Европейско и национални законодателства в областта на киберсигурността

Като се има предвид глобалния и наднационален характер на съвременните информационни системи и технологии, международното сътрудничество има ключова роля за гарантиране на защитата на киберпространството и борбата с киберпрестъпността. Трябва да се подчертае, че за да бъдат мерките за превенция ефективни, международното сътрудничество трябва да се осъществява не само на правителствено ниво, но също и да включва частни субекти и организации като, например, представители на ИТ индустрията, доставчици и разработчици на интернет услуги и продукти и др. Всички те трябва да имат активно участие и да вземат отношение по разработването на една унифицирана, наднационална, законодателна рамка, която да гарантира свободата, защитата и неприкосновеността на информационните технологии и база данни, но и да разписва методически и нормативно мерките и регулациите за превенция и ограничаване на зловредните дейности в Мрежата.

В тази глава ще изследваме европейското законодателство в областта на киберсигурността и електронните услуги. Ще проследим еволюцията в разработването и прилагането на обвързващи и необвързващи нормативни актове в сферата на киберсигурността, за да достигнем и поставим акцент върху революционната **Директива МИС2 (Мрежова и информационна сигурност)**. Модернизираната рамка и регулация, базирана на Директивата за Мрежова и информационна сигурност на ЕС, беше одобрена от Европейският парламент в края на месец ноември 2022 година, с 577 гласа “за” срещу едва 6 “против”.

Разпоредбите по Директива МИС2 влизат в сила за всички държави членки от 2024г. и се възприемат като връх на едно многогодишно сътрудничество между публичните институции и частния сектор за създаването на една актуална, ефективна, устойчива и хармонизирана рамка, защитаваща интересите и правата на фирми и граждани в областта на електронните услуги и кибернетичното пространство, и с поглед към бъдещето.

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

Когато разглеждаме дейността на Европейския съюз в областта на киберсигурността и борбата с киберпрестъпността, трябва се върнем към 90-те години на миналия век, когато биват приети първите необвързващи правни актове, които регулират тези въпроси. Те хвърлят светлина върху предизвикателствата в Мрежата и препоръчват на държавите членки прилагането на подходящи мерки. Посочени са конкретни насоки и предложения за проектите за изменение на националните законодателни актове. Както и разработването на стратегии и планове за действие, подпомагащи подобряването на националните и европейска мрежова сигурност.

Рамково решение 2005/222/ПВР на Съвета на Европа от 24 февруари 2005 г. относно атаките срещу информационни системи в Съюза се явява първият обвързващ правен инструмент на ЕС, чиято цел е да насочи вниманието върху борбата с киберпрестъпленията. Документът дефинира основните понятия за целите на законодателната инициатива („информационна система“, „компютърни данни“, “кибератака”, „киберпрестъпление” и др.) и вменява задължение на държавите членки да разглеждат незаконния достъп до информационни системи и зловредната намеса в мрежите за електронни услуги като наказуемо престъпление. Документът изяснява отговорността на юридическите лица, юрисдикцията, както и описва условията за създаване на център за координация, поддържащ 24-часова услуга, достъпна 7 дни в седмицата, за улесняване на обмена на информация за атаки срещу информационните системи на държавите в Съюза.

Ограниченият брой киберпрестъпления, определени в **Рамково решение 2005/222/ПВР**, заедно с необходимостта от проактивни действия в разпознаването и засичането на нови и по-комплексни киберзаплахи, както и намерението да се адаптират и допълнят разпоредбите към новите инициативи на ЕС в областта на киберсигурността, за да се постигне цялостно регулиране на този предмет, в крайна сметка доведоха до решение за разработване на нов правен инструмент относно киберпрестъпността.

Работата по новия регламент съвпадна с приемането на Договора от Лисабон. В **Директива 2013/40/ЕС** на Европейския парламент и на Съвета

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

на Европа от 12 август 2013 г., засягаща атаките срещу информационните системи, разпоредбите на Рамково решение 2005/222/ПВР в цялостта му бяха потвърдени, но допълнени с редица нови решения. Добавени са нови видове престъпления (например, незаконно прихващане на компютърни данни, атаки с "ботнет", както и престъпления, включващи „инструменти за хакване"). В документа също така са разписани и разяснени дефинициите и правните последствия за извършване на киберпрестъпление от престъпна организация, както е предвидено и в Рамково решение 2005/222, но с много по-строги санкции. Разпоредбите задължават държавите членки да третират подобни случаи и организации с повишена наказателна отговорност. Директивата изяснява още последствията от причиняването на вреди и извършването на престъпление срещу информационните системи със статус на критична инфраструктура. Самите дефиниция и обхват на понятието "критична инфраструктура" са също така изяснени.

Директива 2016/1148 (МИС) на Европейския парламент и на Съвета на Европа от 6 юли 2016 г. прави допълнителни постъпки в посока да подобри мерките за високо общо ниво на сигурност на мрежовите и информационните системи в Съюза. Тя е и гръбнакът на настоящата, актуализирана и допълнена нормативна и регулаторна рамка на ЕС в сферата на киберсигурността (МИС2), за която ще стане дума малко по-късно в тази глава от доклада.

Директивата МИС беше представена като основен елемент и сегмент в Стратегията за киберсигурност на Европа. В амбицията си да повиши защитата на телеинформационните системи, формиращи основата за функционирането на съвременните общества и икономики на страните членки на ЕС, и с мисъл да подобри и обезпечи функционирането на вътрешния пазар на ЕС, Директивата МИС постави акцент върху следните точки:

1. Поставя задължение към всички държави членки да приемат национална стратегия за сигурността на мрежите и информационните системи;

2. Създава контактна група за сътрудничество с цел подпомагане и улесняване на стратегическото взаимодействие и обмена на информация между държавите членки. Създаване на мрежа от екипи за реагиране при

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

инциденти с компютърната сигурност (ЕРИКС), за да допринесе за развитието на доверието между държавите членки и насърчаване на бързо и ефективно оперативно сътрудничество;

3. Установяване на минимални изисквания за сигурност и създаване на протокол за уведомяване от операторите и доставчиците на електронни услуги при засичането и констатирането на компрометиращи дейности;

4. Поставя задължение към държавите членки да определят и посочат националните органи, единните точки за контакт и екипи за реагиране при инциденти с компютърна сигурност (ЕРИКС), както и да вменят и разпределят отговорности и задачи, свързани с обезпечаването на сигурността на мрежите и информационните системи;

Проследявайки развитието на законодателните инициативи на Европейския съюз в областта на мрежовата и информационна сигурност от 90-те години до днес, стигаме и до МИС2. Това е най-новата директива и политика на ЕС в областта на киберсигурността, която всички държави членки се задължават да прилагат от 2024 г. В основата си МИС2 има за главна задача да защити организации от критичната инфраструктура в рамките на ЕС от киберзаплахи и да постигне високо ниво на обща сигурност и хармонизация в ЕС в тази област.

За да постигне тази цел, МИС2 се фокусира върху организации, които предоставят така наречените основни/критични услуги. Това са организации, от които зависи ежедневното и нормално функциониране на обществото, поради което те често са главна мишена за киберпрестъпниците с цел финансова изгода, кражба на данни, изнудване, създаване на хаос и причиняване на граждански вълнения с цел политически дивидент. По-долу ще опишем кои организации са включени в разширения обхват на МИС2 спрямо МИС за учрежденията, предоставящи основни/критични услуги. Директивата включва също така по-строги изисквания за сигурност, по-ултимативни разпоредби за хармонизация с националната нормативна уредба и прилагане на регулациите, по-стриктни задължения за докладване на инциденти, както и по-сериозни изисквания за наказания и правоприлагане.

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

1. Кое изискваше разработването на Директива МИС2?

Макар директивата МИС от 2016 да се явяваше първата всеобхватна политика на ЕС за киберсигурност, тя се нуждаеше от актуализация и адаптация в резултат на нови, нарастващи, непрекъснато еволюиращи и все по-комплексни заплахи за киберсигурността, както и заради проблеми свързани с устойчивостта и съответствието на прилагането на мерките за надзор и контрол в различните държави, което създаде “слаби” връзки и звена и постави сигурността на цялото електронно пространство в Съюза на риск. Трансграничният характер на заплахите продължава да бъде едно от най-големите предизвикателства пред холистичната защита на Европа от киберпрестъпността.

По време на пандемията от Covid-19 светът, също така, преживя безпрецедентна дигитална трансформация на ежедневието и на работния си процес. Това, естествено, доведе със себе си и нарастването на комплексността и на неравномерния начин, по който различните държави и общества използват кибернетичното пространство и се защитават от рисковете и заплахите в него. Иновативността и дързостта на киберпрестъпниците също единствено се подобри.

В отговор на това, Европейската комисия предложи разработването на нова директива. МИС2 цели да запълни пропуските в МИС, като разшири обхвата на доставчиците на основни/критични услуги, като засили изискванията за сигурност в тези организации, адресирайки защитата на веригата за доставки и връзките с трети страни, и увеличи задълженията за докладване на пробиви и инциденти. Целта на този документ е да подготви по-добре организациите в навигирането през комплексния свят на съвременните рискове за киберсигурността.

2. Какъв е обхватът на Директива МИС2 и кои са организациите, предоставящи основни/критични услуги?

МИС2 единствено допълва, пояснява и разширява списъка от МИС с индустриите и организациите, за които ще се прилагат разпоредбите от 2024г. Към средните и големи предприятия от критично важните индустрии (дефинирани от ЕС като такива, които наемат повече от 50 души и чийто годишен оборот надхвърля 10 милиона евро) се добавят, по

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

изключение, и малки предприятия, но само ако същите бъдат определени от отговорния орган на държавата членка да предоставят услуги и продукти, които са от критична важност за функционирането на обществено-социалната и икономическа сфера. Поради тази причина същите биха попаднали в компетентността и обхвата на регулацията, заради потенциалните проблеми, които биха могли да възникнат за страната и обществото, ако въпросните бъдат засегнати от кибератака.

Към настоящия списък от индустрии (здравни грижи, транспортни услуги, банков и финансов сектор, енергетика, дигитална инфраструктура, водоснабдяване) МИС2 добавя към обхвата на Директивата и следните:

а. Електронни комуникации

б. Дигитални услуги

в. Авиоиндустрия

г. Управление на отпадъците (комунални услуги)

д. Хранително-вкусовата промишленост

е. Производство на продукти от критична важност (напр. лекарства)

ж. Пощенски услуги

з. Публичната администрация

МИС2 се фокусира върху операторите на основни услуги – предприятията и организациите, отговорни за поддържането на критичната инфраструктура на дадена страна. Първоначалната директива за МИС създаде сериозни несъответствия в начина, по който държавите членки идентифицираха тези оператори, отчасти в резултат на разграничаването между основни услуги и доставчиците на цифрови услуги. Последните имаха и отделни изисквания за сигурност, съгласно Директивата за МИС, увеличавайки допълнително несъответсвието и непоследователността, тъй като някои държави идентифицираха и дефинираха основните услуги и цифровите услуги по различен начин, създавайки респективно и различни прагове и стандарти за докладване на инциденти.

МИС2 отстранява този проблем, като премахва изцяло разграничението между основни услуги и цифрови услуги и прилага едни и същи правила 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

всички. Поради това фирми, които преди са били считани за доставчици на цифрови услуги, може да се наложи да актуализират своите протоколи за сигурност, за да бъдат в съответствие с общия стандарт МИС2.

3. Какви са санкциите при неспазване на Директива МИС2?

Вероятно най-важното уточнение за организациите, попадащи в обхвата на новата Директива, са по-строгите изисквания за прилагане, които МИС2 въвежда. Тъй като киберсигурността се превръща в ключов проблем, ЕС настоява за спешни действия в своите държави членки, за да осигури устойчивост. Това идва със значителни санкции за онези организации, които не спазват правилата. Те варират от одит на сигурността и предупредителен протокол за следване на препоръките до глоби от 10 милиона евро или 2% от общия световен оборот на организацията – което от тези числа е по-високо. Освен това ръководството на несъответстващите организации, в това число и общинските власти, може да носи лична наказателна отговорност за нарушението на МИС2. В санкциите се допуска дори затвор при особено тежки случаи на неглижираност или несъответствие с разпоредбите за сигурност.

Глобите са сходни с тези при нарушения на Общият регламент за защита на данните (GDPR) и МИС2 трябва да бъде разбиран и третиран от отговорните лица по същия начин. Точно както GDPR създаде нов стандарт за защита на данните, който трансформира начина, по който организациите и служителите мислят и боравят с чувствителната и поверителна информация, така и МИС2 цели да бъде “ракетата-носител” за една всеобхватна трансформация в разбирането за значението на киберсигурността като всеобща задача и кауза, която трябва да се третира със същата сериозност и педантичност, както и GDPR.

4. Какви са основните цели и задачи на Директива МИС2?

Трите основни цели на МИС2 са да повиши устойчивостта на кибернетичното пространство между доставчиците на основни услуги; да оптимизира устойчивостта на киберпространството чрез по-строги изисквания за сигурност и санкции за нарушение; да подобри готовността на ЕС за справяне с кибератаки.

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

1. Увеличаване на киберустойчивостта сред доставчиците на основни услуги

Първата цел е да се увеличи устойчивостта на основните доставчици на услуги в ЕС. Обхватът на доставчиците на услуги, които трябва да отговарят на МИС2, е по-голям от обхвата на оригиналната директива МИС. Всички публични и частни организации в тези категории трябва да спазват едни и същи мерки за киберсигурност. Това гарантира, че ще има по-малко възможност за поява на "слаби" звена и уязвимости в целостта сред доставчиците на критични услуги в ЕС.

2. Оптимизира устойчивостта с по-строги изисквания за сигурност и санкции

Втората цел на МИС2 е за по-добро привеждане на всички отговорни субекти на регулациите в съответствие с изискванията за по-строг контрол за сигурност и санкции за нарушения. Първоначалната директива за МИС позволяваше на организациите да адаптират своето придържане към изискванията за киберсигурност. Въпреки че това им позволи гъвкавост, то също така създаде слаби връзки и доведе до непоследователни нива на сигурност в целия ЕС. Новите изисквания, описани накратко по-долу, са по-добре съгласувани и имат за цел да намалят несъответствията, създадени от директивата МИС.

За да поддържат висок стандарт на сигурност и устойчивост, МИС2 ще изисква от доставчиците на основни услуги да спазват строги изисквания за:

а. Извършване на оценка на риска и наличие на достатъчно надеждни и солидни процеси и политики за съблюдаване сигурността на информационната система;

б. Предотвратяване, откриване и подходящо реагиране на инциденти в срок;

в. Управление на кризи, протокол за действие и оперативна непрекъснатост в случай на голям киберинцидент;

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

г. Гарантиране на сигурността на веригата за доставки или взаимодействието с трети лица и организации, включително доставчици на услуги за обработка или съхранение на данни;

д. Гарантиране на сигурността на собствените мрежови и информационни системи от етапите на разработка до тези на придобиване и поддръжка;

е. Наличие на политики и процедури, които оценяват ефективността на практиките за управление на риска за киберсигурността;

ж. Използване на криптография и криптиране в организационните процеси;

3. Третата главна цел на МИС2 е свързана с подобряването на колективната способност на ЕС да се подготви и да реагира на кибернетични заплахи

Това трябва да бъде постигнато чрез подобряване на комуникацията и обмена на информация между органите на ЕС и държавите членки. МИС2 също така очертава процедурите, които трябва да се следват в случай на мащабен кибер инцидент. Работата и добрите практики по имплементирането на GDPR на наднационално ниво в ЕС със сигурност ще бъдат лакмус и в полза за постигането на тази цел.

Освен това МИС2 ще изисква процес в две стъпки за докладване на инциденти със сигурността пред съответните надзорни органи. Първо, след като дадена организация разбере за инцидент със сигурността, тя трябва да подаде първоначален доклад в рамките на 24 часа след първото узнаване за инцидента. Второ, в този момент за организацията започва да тече срок от един месец, в който да разследва случая и да представи окончателен отчет.

5. Ролята на Агенцията на Европейския съюз за киберсигурност (ENISA) в контекста на законодателните инициативи на Общността в областта на информационната и мрежова сигурност и МИС2

Във връзка с подобряването на колективната способност на Съюза да реагира на опасностите в киберпространството е необходимо да отбележим и един от нейните спомагателни органи. Агенцията на Европейския съюз за киберсигурност (ENISA) е създадена като Европейска агенция за мрежова и информационна сигурност на 15 март 2004 г. с Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета на Европа.

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

МИС2 установява и вменява нови отговорности на ENISA, като по този начин засилва нейната роля и участие в колективния процес. На всеки 2 години ENISA ще има задължението да изготвя подробен доклад за състоянието на киберсигурността в ЕС. Докладът ще има за задача да предостави политически препоръки за справяне с недостатъците и за повишаване на общото ниво на киберсигурност в държавите членки.

ENISA също така ще има участие с препоръки и добри практики при изготвянето от държавите членки на национален план за управление на мащабни кризи и инциденти, свързани с киберсигурността, включително определянето на отговорен компетентен орган (или повече от един). Това е изискване по МИС2, с което вече се запознахме по-назад в доклада. Планът ще трябва да очертае целите и процедурите, които ще бъдат приложени за управление на пробиви в киберсигурността, които имат по-широк ефект върху ЕС. Агенцията също така ще участва в разработването и прилагането на механизма по МИС2 за създаването на партньорска проверка за подобряване на възможностите и политиките за киберсигурност на държавите членки. Експертите, участващи в партньорските проверки, ще трябва да изготвят доклади за констатациите от прегледите, включително препоръки как да се подобрят аспектите на сигурността, обхванати от въпросните прегледи.

МИС2 официално създава и Мрежата на ЕС за връзка при кибернетични кризи (EU-CyCLONe), която ще се координира от ENISA. Целите на EU-CyCLONe са да създаде мрежа, която да позволи сътрудничеството между назначените в държавите членки национални агенции и органи, отговарящи за управлението на киберкризи; да осигурява липсващата свръзка и контакт между техническото и политическо ниво на Европа по обезпечаването на киберзащитата в общността.

ENISA още допринася още за киберполитиката на ЕС като повишава доверието в цифровите продукти, услуги и процеси чрез изготвяне на схеми за сертифициране на киберсигурността. Нейната цел е да предоставя помощ на държавите-членки на ЕС - по отношение на интерпретиране на въпроси, свързани с киберсигурността, и да стимулира развитието на информационното общество.

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

Агенцията си сътрудничи с държавите и органите на ЕС и помага в подготовката за киберпредизвикателствата на утрешния ден. Агенцията работи с организации и предприятия за укрепване на доверието в цифровата икономика, повишаване на устойчивостта на инфраструктурата на ЕС и в крайна сметка за поддържане на цифровата безопасност на гражданите на Съюза. За да постигне целите си агенцията инвестира в обучение, развитие на персонал и структури, и в повишаване на осведомеността. ENISA работи основно в полза на обществени организации като органи, институции и/или децентрализирани органи и агенции на държавите от ЕС. Агенцията също така помага на ИТ индустрията (телекоми, доставчици на интернет услуги и ИТ компании); бизнес общността (особено малкия и среден бизнес); експерти по киберсигурност (например, екипи за реакция при инциденти в киберсигурността); академичните среди, обществеността.

6. Преглед на 10 национални законодателства регулиращи политиките, приоритетите и мерките в областта на киберсигурността: Франция, Германия, Италия, Испания, Нидерландия, Швеция, Естония Белгия, Полша, Румъния (+ България).

За целите на изследването в този доклад набелязахме 10 държави членки на Общността, за да анализираме имплементирането на политиките и мерките им в областта на киберзащитата, с акцент върху публичната администрация и електронните услуги.

За основа на това изследване е полезно да се запознаем първо с главните нормативни уредби, регулиращи тези политики, както и стратегическите приоритети, които са заложени в тях. Важно е да се отбележи, че европейските директиви като МИС2 и GDPR имат правна сила над сходните им национални регулации и/или законодателства.

Директивите МИС2 и GDPR задават минималните задължителни изисквания и критерии за сигурност, като на държавите членки е разрешено да имат по-строги закони и разпоредби, но не и такива с по-ниски изисквания или защитни механизми. В този смисъл, националните закони за киберсигурност трябва да са в съответствие с общоевропейските регулации като Директивите за МИС2 и GDPR. Затова в светлината 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

скорошното им официалното гласуване и ратифициране от Европейския парламент и органите на ЕС, можем да очакваме националните правителства да последват този пример, като актуализират своите нормативни актове в съответствие с европейските. Това се случва и в момента на оперативно ниво, където националните агенции по киберсигурност са в тясно сътрудничество с Агенцията на Европейския съюз за киберсигурност (ENISA) и Европейският съвет за защита на данните (EDPB), които предоставят насоки и подкрепа на държавите членки, за да подготвят актуализирането на нормативните рамки и за да гарантират спазването на законите и разпоредбите за киберсигурност в целия ЕС.

Франция

Основният закон, уреждащ политиките за киберсигурността във Френската Република е „Loi relative à la sécurité intérieure“ (Закон за вътрешна сигурност), който е приет през 2015 г. и актуализиран през 2018 г. Законът изисква от компаниите и публичната администрация да прилагат подходящи мерки за сигурност и защита на личните данни и критичната инфраструктура, и определя глоби и санкции за неспазването им.

Изискванията са за технически мерки като защитни стени и криптиране на чувствителната информация, както и организационни мерки като обучение на служители по политики и процедури. Законът също така изисква от компаниите и публичната администрация да създадат и поддържат протокол и рамка за управление на риска, за да идентифицират и оценят киберинцидентите и да прилагат мерки за смекчаване и минимизиране на тези рискове.

Законът урежда също създаването и статута на ANSSI (Национална агенция за киберсигурност на Франция), която придобива главната отговорност за защита на националната сигурност и критичната инфраструктура срещу кибератаки. Компаниите и публичната администрация са задължени да докладват на Националната агенция за киберсигурност на Франция (ANSSI) за инциденти с информационните и мрежови системи и да уведомяват засегнатите лица, ако техните лични данни са компрометирани от инцидента. Законът също така позволява на ANSSI да разработва и прилага

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

схема за сертифициране на електронни продукти, услуги и процеси, които се считат за ключови за защитата на критичната инфраструктура срещу киберзаплахи.

Друга функция, която агенцията изпълнява, е да координира националната политика по киберзащита и да предоставя препоръки и насоки на националните власти и частния сектор. Освен това има правомощия да извършва одити на киберсигурността и контрол на спазването на закона от страна на организациите и държавната администрация.

Законът определя и налага глоби за неспазване на разпоредбите, като в определени случаи може да наложи, като санкция, затварянето на бизнеси. „Loi relative à la sécurité intérieure“ (Закон за вътрешна сигурност) насърчава повишаването на информираността и осведомеността сред лица и организации за заплахите от киберпрестъпления и методите и успешните практики за превенция.

Законът и неговите разпоредби подлежат на актуализация и развитие заедно с бързия технологичен напредък. За компаниите и публичната администрация е важно да бъдат информирани и в крак с най-новите правни регулации в областта за киберсигурността, европейски и национални, за да осигурят съответствие на процесите и системите си в ултимативната цел да осигурят на клиентите и гражданите си защита срещу киберзаплахите.

Германия

Федерална Република Германия има редица закони, които се занимават с киберсигурността, включително „Bundesdatenschutzgesetz“ (Федерален закон за защита на данните), „Telekommunikationsgesetz“ (Закон за телекомуникациите) и „IT-Sicherheitsgesetz“ (Закон за ИТ сигурността). Заедно те формират основата на политиката за киберсигурност на страната. Тези нормативни актове установяват минималните и/или задължителни изисквания за защита на данните, информационните мрежи и системи, както и определят режима на сигурност на критичната инфраструктура.

Законът за ИТ сигурността (“IT-Sicherheitsgesetz”), приет през 2018 г., определя режима на правомощията и създаването на Федералната служба

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

за информационна защита (BSI), която възприема ролята на германската национална агенция за киберсигурност. Агенцията координира и съблюдава за изпълнението на националната стратегия за киберзащита, като предоставя препоръки на националните власти, публичната администрация и частния сектор. BSI също така предоставя технически насоки и подкрепа на организациите, за да приложат подходящи мерки за сигурност.

Законът за ИТ сигурността има за цел да подобри защитата на ИТ системите на федерално ниво, които се считат за базови за функционирането на критичната инфраструктура, както и цялостно да спомогне засилването и подобряването на киберсигурността на германската икономика и публичния сектор. Законът изисква операторите на критична инфраструктура и данни да предприемат адекватни мерки за сигурност, да назначат служител по ИТ сигурността и да докладват инциденти на Федералната служба за информационна сигурност (BSI).

Федералният закон за защита на данните определя правната рамка за защита на данните в Германия и допълва Общия регламент за защита на данните на ЕС (GDPR). Прилага се за събирането, обработката и съхранението на лични данни, което включва изисквания за сигурност на данните и докладване на инциденти. Особено актуален е за публичната администрация във Федералната република.

Федералният закон за телекомуникациите регулира телекомуникационния сектор и изисква от доставчиците на услуги да предприемат конкретни технически мерки за сигурност, за да защитят своите мрежи и услуги от неоторизиран достъп, манипулиране и смущения.

Във всеки един от гореспоменатите закони са определени глобите и наказанията при неспазване на разпоредбите. В случай на сериозни провинения организациите могат да бъдат изправени пред санкции като временно или постоянно затваряне на бизнеса.

Италия

Основният закон на Република Италия за киберсигурността е „Codice della sicurezza digitale“ (Кодекс за цифрова сигурност), който е приет през 2018 г., за да допълни и актуализира предишното законодателство на страната в

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

областта на киберзащитата и киберпрестъпленията. Нормативната уредба установява изискванията за защита на личните данни и критичната инфраструктура, а също така определя режима на санкциите при неспазване.

Законът изисква компаниите и публичната администрация да прилагат подходящи мерки за сигурност и защита на личните данни и критичната инфраструктура и да извършват редовни оценки на сигурността, като докладват за киберинциденти на Националния център за киберсигурност (NCC). Това е агенцията, която координира дейностите по киберсигурност в страната, изготвя препоръки на националните органи и частния сектор и насърчава осведомеността по темата киберсигурност сред лица и организации.

Законът насърчава споделянето на информация и сътрудничеството между правителствени агенции, публични органи, частния сектор и международни партньори с цел подобряване на киберсигурността и улесняване на откриването и реагирането на киберзаплахи. Законът също така предвижда създаването на специализирани звена за борба с киберпрестъпността и установяването на престъпления и наказания, свързани с киберпрестъпления.

Някои от техническите изисквания за защита на системите и базата данни за организациите от публичния и частен сектор, упоменати в закона, са:

а. Криптиране на лични данни и чувствителна информация;

б. Внедряване на механизми за контрол на достъпа като, например, двуфакторно удостоверяване на идентичността;

в. Редовни оценки на сигурността и тестове за проникване;

г. Изпълнение на планове за реакция при инциденти и докладване на кибер инциденти към Националния център за киберсигурност (NCC);

д. Съответствие с международните стандарти за сигурност като ISO/IEC 27001;

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

е. Публичните административни органи трябва да назначат длъжностно лице по защита на данните и да разполагат с подробен план за действие и управление на инциденти, с оценка на риска;

Като цяло, италианският закон и политика за киберсигурност се фокусират върху защитата на критичната инфраструктура, включително енергийния и транспортния сектор и цифровата икономика. Насърчават прилагането на подходящи мерки за сигурност, докладването на киберинциденти и повишаването на осведомеността по темата превенция и киберзащита сред организации и лица. Законът също така акцентира върху защитата на личните данни и предоставянето на инструменти за борба с киберпрестъпността.

Испания

Основните нормативни документи, които установяват изискванията за защита на киберпространството, данните, дигиталните услуги и мрежата в Кралство Испания, са „Ley Orgánica de Protección de Datos“ (Закон за защита на данните) и „Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico“ (Закон за информацията в обществените услуги и електронната търговия).

В допълнение, Кралският декрет - закон за защита на критичната инфраструктура - упоменава регулаторната рамка за превенция срещу кибератаки срещу жизненоважните компоненти на националната мрежа. Той определя изискванията и задълженията на организациите, управляващи тези инфраструктури.

Органът, който отговаря за защитата на испанската национална сигурност в киберпространството, е Националният криптологичен център (CCN). Той координира националната киберотбрана, предоставя препоръки на националните органи и частния сектор, насърчава обмена на информация и сътрудничеството между секторите и подпомага с ресурси и обучение повишаването на осведомеността за киберсигурността сред лица и организации.

Ключови практически изисквания към частния и публичния сектор, залегнали в гореспоменатите закони, са:

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

а. Уведомяване за нарушения на сигурността: От компаниите и публичната администрация се изисква да уведомяват съответните органи за всякакви нарушения на сигурността, които биха могли да компрометират личните данни;

б. Прилагане на мерки за сигурност: Компаниите и публичната администрация трябва да прилагат подходящи технически и организационни мерки за защита на личните данни от неоторизиран достъп, подмяна и унищожаване;

в. Минимизиране на данните: Компаниите и публичната администрация трябва да събират само минималното количество лични данни, необходими за конкретната цел, за която се обработват;

г. Запазване на данни: Компаниите и публичната администрация трябва да съхраняват лични данни само толкова дълго, колкото е необходимо за конкретната цел, за която се обработват;

д. Прозрачност: Компаниите и публичната администрация трябва да информират лицата за събирането, използването и споделянето на техните лични данни, включително техните права във връзка с тези данни;

е. Получаване на съгласие: Компаниите и публичната администрация трябва да получат изрично съгласие от физически лица за определени видове обработка на данни като ,например, маркетингови съобщения;

ж. Одити и сертификати за сигурност: Компаниите и публичната администрация се насърчават да преминат през одити за сигурност и сертифициране, за да демонстрират съответствието си с изискванията за киберсигурност.

Политиката за киберсигурност на Испания включва редица технически и стратегически приоритети, които имат за цел да подобрят сигурността на цифровата инфраструктура на страната и да защитят нейните граждани и организации от киберзаплахи. Някои от основните стратегически приоритети, залегнали в нормативната база на страната, са:

1. Управление на инциденти в киберсигурността: Испанското правителство има за цел да създаде национална рамка за управление на инциденти, която да помогне на организациите и публичната администрация да

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

реагират бързо и ефективно на инциденти в кибернетичното пространство и да минимизират въздействието от пробиви в сигурността.

2.Киберсигурност на критичната инфраструктура: Испанското правителство поставя висок приоритет върху защитата на критичната инфраструктура на страната от кибератаки, като това се отнася до структурите на общинската власт, електрическата мрежа, финансовата система и транспортните мрежи.

3. "Облачна" сигурност: Испанското правителство насърчава използването на "облачни" изчислителни системи в публичния и частния сектор, но със силен акцент върху прилагането на подходящи мерки за сигурност и защита на данните и мрежите.

4. Сигурност на Интернет на нещата (IoT): Испанското правителство е наясно с потенциалните рискове на IoT устройства и насърчава използването на най-добрите практики за сигурност при разработването и внедряването на тези устройства.

5. Сигурност на системите за индустриален контрол: Испания също има специален интерес към сигурността на системите за индустриален контрол и работи активно за подобряване на сигурността им и намаляване на риска от кибератаки срещу мрежите, свързани с важни промишлени процеси.

6. Умения за киберсигурност: Испанското правителство инвестира в образование и обучение по киберсигурност, за да изгради силна работна сила, която може да се защитава от киберзаплахи.

<u>Нидерландия</u>

В Кралство Нидерландия действат редица специфични закони, уреждащи нормативният статус и изисквания в областта на киберсигурността и личните данни.

„Wet bescherming persoonsgegevens" (Закон за защита на данните) прилага съответствие с GDPR на ЕС и определя изискванията за защита на поверителната и лична информация, включително сроковете и способите за задържане на данни, както и докладването на инциденти.

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

“Wet elektronische handtekening” (Закон за електронните подписи) упоменава режима за имплементиране в работата на електронното правителство на електронните подписи и електронните транзакции и установява законови изисквания за тяхното използване.

“Telecommunicatiewet” (Закон за телекомуникациите) регулира телекомуникационния сектор и изисква от доставчиците на услуги да предприемат подходящи мерки за сигурност, за да защитят своите мрежи и услуги от неоторизиран достъп, манипулация и пробиви.

Нидерландското правителство има засилен фокус върху борбата с киберпрестъпността и отделя значителни ресурси за това усилие. Това включва отдела за киберпрестъпления към Националната полиция и Националния отдел за киберпрестъпления към прокуратурата, които отговарят за разследването и преследването на случаи на киберпрестъпления.

Нидерландското правителство също поставя силен акцент върху защитата на личните данни на гражданите и важността на реакцията при инциденти и управлението на риска. Центърът за киберсигурност в Нидерландия (NCSC-NL) отговаря за защитата на националната сигурност на страната и критичната инфраструктура срещу кибератаки. Той координира националната киберотбрана и стратегия, предоставя препоръки на националните органи и частния сектор и насърчава осведомеността за киберсигурността сред лица и организации.

Друг важен аспект от нидерландската политика за киберсигурност е ролята на частния сектор в защитата на националната сигурност. Правителството насърчава частния сектор да споделя информация със съответните органи за инциденти, заплахи и уязвимости. Те също така активно участват в публично-частни партньорства с компании и организации за повишаване на осведомеността и за разработване на механизми за реагиране.

По отношение на приоритетите нидерландската политика за киберсигурност е фокусирана върху защитата на критичната инфраструктура, на мрежите и системите на общинските власти, както и на енергийния и транспортни сектори и цифровата икономика. Освен това нидерландското правителство поставя значителен акцент върху

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

международното сътрудничество с цел ефективна борба с киберпрестъпността. NCSC-NL работи в тясно сътрудничество с други национални и международни партньори за споделяне на информация и най-добри практики с цел подобряване на устойчивостта на страната срещу кибератаки.

Естония

Малката балтийска държава е в центъра на вниманието на европейската политика в областта на киберсигурността още от 2007 година, когато претърпява една от най-широкомащабните кибератаки, насочена към публичния сектор и медиите, за която се смята, че е организирана от чужда държава (Руската Федерация). Случаят на Естония е един от първите примери за кибервойна, в резултат на който страната се превърна във флагман на борбата срещу заплахите в електронната мрежа и в една от най-напредничавите държави в областта на цифровизацията и киберсигурността. Балтийската държава е известна с иновативния си подход към защитата на дигиталните услуги и среда, със силен акцент върху използването на технологии за защита на критичната инфраструктура и услуги.

Правителството на Естония инвестира значителен ресурс в изграждането на своята цифрова инфраструктура и създаването на култура, която насърчава използването на технологии във всички аспекти на живота. Това доведе до високо ниво на цифрова грамотност сред населението и силна екосистема от технологични компании, които са подкрепени от една солидна законодателна и регулативна рамка в областта на електронните услуги и превенцията на злонамерена дейност в интернет.

Естония има редица закони и разпоредби, насочени към киберсигурността, включително „Закона за защита на личните данни“ и „Закона за услугите на информационното общество“, който регулира сектора на електронните комуникации и изисква от доставчиците на услуги да предприемат конкретни технически и оперативни мерки за сигурност, за да защитят своите мрежи и услуги от неоторизиран достъп, манипулиране и кибератаки.

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

"Законът за мрежите и информационните системи" е предназначен да подобри сигурността на критичната инфраструктура и цифровите услуги.

По отношение на борбата с киберпрестъпността Естония постигна значителни успехи в предотвратяването на киберпрестъпността чрез своята така наречена Лига за киберзащита. Тя представлява мрежа от организации от публичния и частния сектор, които споделят информация и най-добри практики за киберсигурност.

Органът за информационна и системна сигурност (RIA) е националната агенция за киберсигурност на Естония. Той координира националната киберзащита и предоставя препоръки на националните власти и частния сектор. RIA също така предоставя технически насоки и подкрепа на организациите, за да приложат подходящи мерки за сигурност. Към агенцията действа Компютърният екип за спешно реагиране на Естония (CERT-EE), който отговаря за реакцията при инциденти и координира дейностите по киберсигурност. Отделно действат специални звена за киберпрестъпления в естонската полиция и Гранична охрана.

Швеция

И в Кралство Швеция, както в партньорските държави от Общността, действат редица нормативни актове, които се занимават с киберсигурността и неприкосновеността на личната информация. Те поставят изискванията за спазване и уреждат случаите, в които законът може да налага санкции. Сред основните правни документи са „Personuppgiftslagen" (Закон за личните данни) и „Lag om elektronisk kommunikation" (Закон за електронните комуникации).

Санкциите за неспазване на законодателството в областта на мрежовите и информационни системи варират в зависимост от сериозността на инцидента и нивото на сътрудничество на провинилата се организация с властите. Шведският надзорен орган може да наложи административни глоби до 10 милиона шведски крони (приблизително 1,2 милиона долара) за неспазване на закона. Освен това агенцията може да налага глоби за неотчитане на инциденти и за непредприемане на подходящи мерки за управление на рисковете за мрежовите и информационните системи. От организациите на публичния и частен сектор може също така да се изисква

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

да приложат конкретен план за действие за справяне с проблеми, свързани с несъответствие. В случай на тежки нарушения прокуратурата може още да отнесе случая до съд и на отговорното лице да бъдат наложени санкции, включително затвор.

Законът за мрежите и информационните системи е предназначен да подобри сигурността на критичната инфраструктура и цифровите услуги и изисква от операторите на основни услуги, сред които и публичната администрация, както и доставчиците на цифрови услуги, да предприемат конкретни технически и оперативни мерки за сигурност, да докладват инциденти и да назначат лице, отговорно за имплементиране на политиките по киберзащитата.

Законът за електронните комуникации регулира сектора на електронните комуникации и изисква от доставчиците на услуги да предприемат технически и оперативни мерки за сигурност, за да защитят своите мрежи и услуги от неоторизиран достъп и кражба на данни.

По отношение на борбата с киберпрестъпленията, шведското правителство има специално звено за киберпрестъпления в рамките на Националната полиция, което отговаря за разследването и наказателното преследване на случаи на киберпрестъпления.

Правителството също така поставя силен фокус върху предотвратяването на киберпрестъпления чрез образователни кампании за информиране на обществеността. Правителството участва активно в публично-частни партньорства с компании и организации от ИТ индустрията за повишаване на осведомеността, предотвратяване на киберпрестъпления и разработване на механизми за реагиране. Шведският национален център за киберсигурност отговаря за стратегическата координация на защитата на националната сигурност на страната в киберпространството. Агенцията също така предоставя технически насоки и подкрепа на организациите и публичната администрация, за да приложат подходящи мерки за превенция.

Шведското правителство дава приоритет на защитата на критичната инфраструктура, дигиталните услуги и личните данни, международното сътрудничество и обмен на информация с партньорски агенции и служби.

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

Полша

Полша има редица закони и разпоредби, които се отнасят до киберсигурността, защитата на личните данни, критичната инфраструктура и мрежовата и системна сигурност на страната. Националният център за киберсигурност координира националната стратегия за киберзащита и предоставя препоръки на националните власти и частния сектор. Екипът за компютърно реагиране при извънредни ситуации в Полша отговаря за реакцията при инциденти и надзирава дейностите по защита на дигиталното пространство. По отношение на борбата с киберпрестъпленията, полското правителство разполага със специално звено и в полицията, което отговаря за разследването и преследването на случаи и лица свързани с организирането и извършването на зловредна дейност в дигиталната среда.

Основните разпоредби на полските закони в областта на киберсигурността включват:

Закон за защита на личните данни: Прилага Общия регламент за защита на данните на ЕС (GDPR) и определя изисквания за защита на личната информация, включително изисквания за сигурност на данните и докладване на инциденти.

Закон за защита на критичната инфраструктура: Установява регулаторната рамка за защита на критичната инфраструктура срещу кибератаки и определя изискванията и задълженията на организациите, управляващи тази инфраструктура.

Закон за националната система за киберсигурност: Урежда защитата на информационните системи и услуги от обществено значение и създава система за защита срещу киберзаплахи.

Най-важните аспекти на полската стратегия за киберсигурност, залегнали в нормативната база на страната, включват:

1. Подобряване на способностите на Националната система за киберсигурност, която отговаря за защитата на критичната инфраструктура и правителствените мрежи на Полша, да открива, предотвратява и реагира на киберинциденти. Това включва прилагане 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

високи технологии като машинно обучение и изкуствен интелект. Също стимулира укрепването на споделянето на информация и сътрудничеството между правителствените агенции и частния сектор;

2. Подобряване на готовността и устойчивостта на киберсигурността на публичната администрация и на частния сектор с акцент върху малките и средните предприятия. Това включва мерки за повишаване на осведомеността за рисковете за киберсигурността и най-добрите практики, както и предоставяне на инструментите и ресурсите, от които се нуждаят, за да се защитят. Правителството също така цели да насърчи разработването на решения за киберсигурност от полски компании и използването на тези решения от частния сектор;

3. Разработване на квалифицирана работна сила в областта на киберсигурността чрез програми за образование и обучение. Стратегията цели да увеличи броя на хората с умения в сферата на киберсигурността чрез инициативи като програми за образование и обучение, стажове и стипендии, както и чрез предлагане на директни стимули за компаниите, които наемат специалисти по киберсигурност;

4. Укрепване на международното сътрудничество в областта на киберсигурността включително чрез участие в Стратегията за киберсигурност на Европейския съюз и Центъра за върхови постижения на НАТО за съвместна киберотбрана;

5. Редовно актуализиране и укрепване на законодателството с цел осигуряване на ефективна защита срещу киберзаплахи;

6. Разработване на механизъм за бързо реагиране при инциденти за справяне и смекчаване на кибератаки;

<u>Белгия</u>

Основното законодателство на Кралство Белгия по отношение на киберсигурността е “Законът от 13 март 2018г.”, който покрива защитата на съхранението и обработката на лични данни. Това е белгийското прилагане на Общия регламент за защита на данните на ЕС (GDPR). Прилага се както за организации, работещи в рамките на ЕС, така и за организации

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

извън ЕС, които обработват лични данни на физически лица в ЕС, в това число се отнася и за публичната администрация.

Основните регулаторни изисквания към частния и публичния сектор по отношение на превенцията на киберсигурността съгласно GDPR са:

1. Организациите трябва да назначат длъжностно лице по защита на данните, ако са частна или публична компания и ако основните им дейности се състоят от обработка на чувствителни лични данни в голям обем;

2. Организациите трябва да прилагат подходящи технически и организационни мерки за защита на личните данни от неоторизиран достъп, подмяна, разкриване или унищожаване. Тези мерки трябва да вземат предвид състоянието на техниката, разходите за изпълнение и естеството, обхвата, контекста и целите на обработката;

3. Организациите трябва да гарантират, че всички трети страни, които ангажират да обработват лични данни от тяхно име (като доставчици на облак услуги или обработващи данни трети фирми), предоставят достатъчни гаранции за сигурност и спазват GDPR регламента;

4. Организациите трябва да докладват за нарушения при съхраняването на данните на съответните органи и на засегнатите субекти на данни без неоправдано забавяне;

5. Организациите трябва да извършват редовни оценки на риска, за да осигурят сигурността на своите дейности по обработка на лични данни и да идентифицират и адресират всички уязвимости;

6. Организациите трябва да могат да демонстрират съответствие с GDPR, например, като поддържат записи на своите дейности по обработка на данни;

Важно е да се отбележи, че за определена критична инфраструктура и за определени видове компании белгийското законодателство добавя задължения за киберсигурност извън GDPR. Същите са описани в законодателството за мрежите и информационните системи.

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

Както вече разгледахме по-назад в доклада, Директивата за мрежовите и информационните системи (МИС), в първата си версия, осигурява регулаторната рамка за киберсигурност на ЕС. Директивата за МИС беше приета през 2016 г. и държавите членки, включително Белгия, бяха задължени да я транспонират в националното си законодателство до май 2018 г.

В Белгия Директивата се прилага за „оператори на основни услуги“ и „доставчици на цифрови услуги“ от 2 юни 2018 г. и касае сигурността на мрежите и информационните системи. Струва си да се отбележи, че понятието „оператори на основни услуги“ е дефинирано в белгийското законодателство и включва доставчици на критична инфраструктура и услуги като енергия, транспорт и здравеопазване, банки и финанси, но също така и публичната администрация, както и доставчици на цифрови услуги като услуги за изчисления в облак, търсачки и платформи за електронна търговия.

Основните разпоредби и изисквания в белгийското законодателство за МИС са:

а. „Операторите на основни услуги“ са длъжни да уведомяват „Екипа за компютърно реагиране при спешни случаи“ за инциденти, които имат значително въздействие върху непрекъснатостта на основната услуга, която предоставят. Те трябва да направят това възможно най-скоро, но най-късно до 12 часа след откриването на пробив в системата.

б. От „операторите на основни услуги“ и „доставчиците на цифрови услуги“ се изисква да предприемат конкретни технически и организационни мерки, за да осигурят ниво на сигурност, подходящо за риска на мрежовите и информационни системи (МИС), които управляват. Те трябва също така да предприемат мерки за докладване на инциденти и мерки за сътрудничество с екипите за реагиране при инциденти.

в. От „доставчиците на цифрови услуги“ се изисква да уведомяват „Органа за защита на данните“ на Белгия, както и засегнатите субекти на инцидента с поверителната информация в случай на висок риск за правата и свободите на въпросните лица.

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

Федералната агенция за сигурност на информационната система (FASI) е националният орган за киберсигурност на Белгия. Той координира националната стратегия в областта на киберзащитата и предоставя препоръки на националните власти и частния сектор. Той също така предоставя технически насоки и подкрепа на организациите и публичния сектор, за да приложат подходящи мерки за сигурност.

Румъния:

Република Румъния е внедрила Директивата на ЕС за мрежите и информационните системи (МИС) в националното си законодателство чрез Наредба №. 13/2019. Основните разпоредби на румънското законодателство за МИС са:

1. Публичата администрация и частните компании, които предоставят основни услуги като енергия, транспорт, здравеопазване и водоснабдяване, се считат за „оператори на основни услуги“ и са подчинени на законодателството на МИС.

2. Операторите на основни услуги и доставчиците на цифрови услуги са длъжни да предприемат подходящи технически и организационни мерки, за да гарантират сигурността на своите мрежови и информационни системи, включително докладване на инциденти и сътрудничество с екипи за реагиране при инциденти.

3. Операторите на основни услуги са длъжни да уведомяват Екипа за компютърно реагиране при извънредни ситуации в Румъния и Националния орган за управление и координация на защитата на инциденти, които имат значително въздействие върху непрекъснатостта на основната услуга, която предоставят. Правителството има правомощието да налага глоби за неспазване на законодателството по Директивата МИС.

4. Компаниите и органите трябва да разполагат с план и протокол, да демонстрират съответствие в прилагането на процедурите за реагиране при инциденти и уведомяване за нарушения, трябва да могат да идентифицират и оценяват рисковете за своите мрежи и информационни системи и трябва да могат да реагират бързо и ефективно на всякакви инциденти.

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

Румънското правителство е разработило и стратегия за киберсигурност в публичната администрация, която определя целите, приоритетите и действията, които трябва да бъдат предприети за подобряване на киберсигурността в държавния сектор. Стратегията има за цел да засили устойчивостта на публичната администрация срещу кибератаки, да защити чувствителната информация на гражданите и да осигури непрекъснатост на публичните електронни услуги. В тази връзка:

а. Стратегията и законът за националната киберсигурност изискват от публичната администрация да докладва за киберинциденти на Националния орган за киберсигурност и да си сътрудничат с тях в процеса на реакция при инциденти.

б. Националният орган за киберсигурност провежда редовни одити на киберсигурността в публичната администрация, за да оцени готовността за реакция и ефективността на техните мерки, както и да идентифицира потенциални уязвимости.

в. Националният орган за киберсигурност провежда програми за обучение и повишаване на осведомеността, знанията и уменията на служителите в публичната администрация в сферата на киберсигурността.

В обобщение, румънското правителство поставя значителен акцент върху киберсигурността на публичната администрация и е приложило набор от мерки и политики за подобряване на сигурността на мрежите, системите и данните в публичния сектор чрез прилагане на подходящи мерки за сигурност, докладване на киберинциденти и насърчаване на осведоменост за киберсигурността сред служителите. Правителството също така приоритизира провеждането на редовни одити на киберсигурността и насърчава участие в публично-частно партньорство за по-добра устойчивост срещу кибератаки.

<u>България:</u>

В заключение, макар тема на този доклад да е изследването на нормативната уредба в сферата на киберсигурността на 10 държави-членки от Общността, е разумно също така да отделим внимание и на българската правна рамка.

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

С цел повишаване на институционалната ангажираност в съответствие с останалите страни от ЕС, и за да осигури по-ефективно осъществяване на политиките в сферата на е-управлението и киберсигурността, на 13 декември 2021г., с Решение на Народното събрание, бе създадено Министерството на електронното управление, чиято основна задачи е в организацията, обезпечаването, управлението и контрола на дейностите по киберсигурността на критичната инфраструктура и обекти в страната.

Правната рамка, чрез която то осъществява дейността си, е Законът за киберсигурността, приет от Народното събрание на 31 октомври 2018 г. и обнародван в брой 94 на Държавен Вестник на 13 ноември 2018г. В своята същност, Законът транспонира Директива 2016/1148 на Европейския парламент и на Съвета на Европа от 6 юли 2016 година. Той е внимателно съобразен с българската кибер-екосистема, нейните рискове, заплахи и предизвикателства, като взаимства от най-успешните мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

Този закон урежда дейностите по двете главни направления:

1. Управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността;

2. Предприемане и имплементиране на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност;

С този закон се определят още и правомощията и функциите на компетентните органи в областта на киберсигурността, както и предвидените санкции за нарушения, протоколите за уведомяване на инциденти и сроковете затова, на база класификацията на киберпробива и въздействието му върху непрекъснатостта на системите.

IV. Представяне на добри практики в сферата на киберсигурността на публичната администрация

В тази глава ще се запознаем с добрите практики от сферата на киберсигурността, които всяка една публична администрация може да приложи в оперативния си процес, за да гарантира ефективна защита 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

своите мрежови и информационни системи, а също и на поверителността на данните на потребителите.

Надеждното функциониране на общинските услуги, в това число и електронните, е от ключово значение както за местните власти, така и за гражданите, които очакват и изискват качествени, достъпни и навременни услуги в замяна на плащането на данъци. Потенциална кибератака срещу основните услуги и критичната инфраструктура на публичната администрация може да окаже разрушителен ефект върху устоите на местното управление и доверието между местната власт и нейните граждани.

Общинските власт и услуги са "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, по дефиниция, общинските власти са по-слабо подготвени за защита от кибератака. Те се определят като сравнително лесна "жертва" 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 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.

Предизвикателство за киберзащитата се явява и законовото изискване общинските и държавните администрации да предоставят прозрачност и отвореност на информацията и дигиталните услуги за целите на електронното и "отворено" правителство.

Европейската агенция за киберсигурност (ENISA) установява най-добрите практики за защита на мрежовите и информационни системи чрез изследване на текущи европейски и световни инициативи, които са се доказали като адекватни и ефективни в насърчаването на сигурна киберсреда. Важно е обаче да се отбележи, че иновативността и комплексността на кибератаките изпреварват законодателните и регулаторни мерки в тази сфера, затова е необходимо същите, както 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

респективно, насоките и добрите практики в противостоенето на зловредната дейност в киберпространството, да бъдат редовно и навременно актуализирани. Глобализацията и свързаността на интернет пространството изискват повишен акцент върху необходимостта от последователни и холистични, наднационални подходи към предизвикателствата в киберпространството.

В тази глава, условно, ще разделим изследването на добрите практики в две посоки - на **стратегически** и на такива с **практическо** приложение.

При разработването на правилна **стратегия** за борба с киберсигурността и за да бъдат максимално ефективни приложените мерки, публичната администрация трябва:

1. Да познава добре спецификите на своята среда. Всяка местна власт е малко или много уникална по отношение на потенциалното въздействие на различните видове рискове. Добрата стратегия и добрата отправна точка за планиране се състоят в доброто разбиране на тези специфики. 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.

2. Да изготви 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,

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 самата мрежова и информационна система в 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.

3. Да формулира и обясни ясно целите и задачаите: При разработването на всеобхватна киберстратегия е важно визията и целите ѝ да бъдат правилно и ясно формулирани и още по-правилно 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-ключовия фактор в борбата с киберпрестъпността. С други думи, ако публичната администрация не предприеме необходимите усилия да разясни на своите служители защо изпълнението на стратегията и мерките, заложени в нея, са от критична важност, тя най-вероятно няма да пожъне успеха, на който се е надявала.

Планът за изпълнение трябва да включва 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

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

отделният потребител знае как да се защити от зловредните практики в дигиталната среда, които, потенциално, могат да засегнат не само публичната администрация по места, а и националната киберсигурност на цялата държава.

4. Киберсигурността не е задължение на един човек: Императив на всяка стратегия за киберсигурност трябва да бъде убеждението, че киберсигурността е обща отговорност. Тя не е отговорност на една агенция, организация или физическо лице, а 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.

Отглеждането на една цялостна екосистема от субекти и обекти със сходно ниво на култура и компетентност в областта на киберсигурността задължително ще доведе до ползотворни резултати, изразяващи се в по-добре подготвена и защитена среда от рисковете на киберпространството.

5. Партньорство и сътрудничество: Както вече научихме, никой субект, компания, частна или публична организация не е защитен остров от рисковете на дигиталната среда. Напротив, абсолютно всеки, който има достъп до електронните мрежи и услуги, е изложен на опасност от зловредно проникване и дейност. Също така научихме, че превенцията на киберпрестъпността е обща мисия и кауза, в която общото е много по-силно от частното. Затова е естествено част от стратегията за киберсигурност на една публична администрация да бъде и в насърчаването на партньорство с частния сектор и националните органи.

Местните власти могат да се възползват от сътрудничеството с частния сектор, като използват опита и “ноу-хау”-то на индустрията. Това включва придобиването на готови продукти и услуги с високи и проверени нива на сигурност, както и да се възползват от знанията и компетентността 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

компаниите. Освен това публично-частното сътрудничество е важно за защитата на критичната инфраструктура, тъй като по-голямата част от нея се притежава и управлява от частни субекти. Следователно те трябва да участват активно в процеса на планиране, насочен към защита на националната критична инфраструктура срещу киберзаплахи. Включването на възможно най-много заинтересовани страни в процеса на разработване на стратегията за киберсигурност е от съществено значение. В допълнение, включването на всички съответни заинтересовани страни гарантира, че те допринасят със своите експертни познания и опит за постигането на по-висок процент на успех в превенцията от кибератаки.

Публичната администрация също трябва да насърчава към инвестирането в научноизследователска и развойна дейност на местна почва. Това е от съществено значение за разработването на нов инструментариум за възпиране и защита от киберзаплахи, ползите от които са за най-широк кръг от хора и институции.

За да преведат стратегическите насоки към изпълнение на практически задачи, експерите по сигурността предлагат богат набор от ефективни мерки за превенция на рисковете в дигиталната сфера.

Тяхното **практическо приложение** ще обобщим и разгледаме по-долу.

1. Оценка на уязвимостите на системите чрез инвентаризация и актуализация. Публичната 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, 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. Организациите от публичния сектор трябва да гарантират, че целият им компютърен и дигитален набор се актуализира редовно с най-

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

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: Публичната администрация трябва да изисква от служителите си да прилагат стриктна политика за силни пароли, за да 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. 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.

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 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

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

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 достъпна бюджетно и изпълнима мярка, която същевременно оказва надеждна защита за акаунтите и поверителната информация, съдържаща се в тях.

4. Криптиране на информацията: Публичната администрация е натоварена с отговорната задача да борави със и да съхранява 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, 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 многофакторна 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 добра 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.

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

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. Архивирането е най-базовият и евтин начин, по който местната власт може да предпази мрежите си от рансъмуер, който, както научихме по-назад в доклада, е сред най-разпространените и чести метод за кибератаки.

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

6. 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", да 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 мениджмънт 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 публичната администрация да проверява и контролира дали външните доставчици на ИТ услуги спазват всички приложими закони и регулации за сигурност на данните. Един начин това

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

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, публичната 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.

7. Кризисен план за действие: 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.

Времето за изготвяне и утвърждаване на план за реагиране трябва да е 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 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

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 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.

8. Приложете ориентиран към хората подход за сигурността: Служителите могат да бъдат най-големия риск за сигурността на една общинска администрация или 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, важност и значение в този процес. От ключово значение е те да разберат и възприемат защо спазването на правилата за киберсигурност е така 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 важно да им се обясни, че техните действия или бездействия имат резултат и цена. Всеки един служител 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 киберпространството 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 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.

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

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.

9. Защитете достъпа на информацията си 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".

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 публичната администрация е важно 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.

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

а. Обучението за 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

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

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.

10. 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 и 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.

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-

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

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.

11. 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 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.

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.

12. 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

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

голям брой субекти и обекти за системата за защита имат няколко съществени недостатъка.

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.

13. 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 публичната администрация да бъде в крак с най-новите разработки, доклади и препоръки и да има 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.

В обобщение на добрите практики за киберзащита, които може да имплементира в организационния си процес общинската власт, и преди да преминем към разглеждането им в контекста на 10-те набелязани държави членки на ЕС, можем да заключим следното.

Докато киберсигурността продължава да представлява значително предизвикателство за всички нива на държавната администрация, тя може да си послужи от опита и експертизата на ИТ индустрията, която, по

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

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.

Публичната 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.

Естония – Дигитално общество и киберсигурност за пример на цяла Европа

За да се поучим от най-добрите практики в сферата на киберсигурността на електронните услуги, предоставяни от публичната администрация на европейско ниво, е необходимо да разгледаме в детайли примера "Естония". Малката балтийска държава, неслучайно наричана "Е-стония", е абсолютният шампион на Европа, що се касае до трансформацията и дигитализацията на обществото, на електронните услуги и на местната власт. Страната е също така неоспоримият европейски лидер в разработването на напредничави политики за справяне с предизвикателствата на киберсигурността, както и в имплементирането на ефективни и ефикасни мерки за защита на критичната си инфраструктура и електронни услуги от опасностите на киберпространството.

Достатъчно красноречив е фактът, че (почти) всяка друга европейска държава се уповава на опита и следва добрите практики на Талин в сферата на киберзащитата. Балтийските експерти по киберсигурността днес съветват редица държави и правителства по въпросите на мрежовата и информационна защита. Страната е подписала рамкови споразумения 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

обучение и сътрудничество в сферата на киберсигурността с Австрия, Люксембург, Германия, Франция, Полша, Литва, Латвия, Южна Корея и НАТО. Друг показателен факт за ролята и значението на Талин в тази сфера е, че през декември 2016 г. НАТО организира най-голямата си конференция по киберзащита именно в Естония. Наречено “Cyber Coalition 2016”, тридневното събитие привлече повече от 700 киберзащитници и правни експерти, правителствени служители, военни, академици и представители на индустрията.

Република Естония е на път да се превърне в първото напълно цифрово общество. Като нация с най-голям цифров актив в света, повечето държавни функции работят онлайн – включително здравеопазване и гласуване. Страната е почти изцяло безкасова и безкешова. За да оценим степента на цифровизация на естонското общество в контекста на използването и наличието на електронни услуги в публичната администрация, можем да си послужим със следните цифри, източник на които е естонското правителство:

- 99% от общо 2700-те държавни, административни услуги са налични онлайн (2022г.)

- 89% от естонските данъкоплатци предпочитат да си плащат онлайн (2021г.)

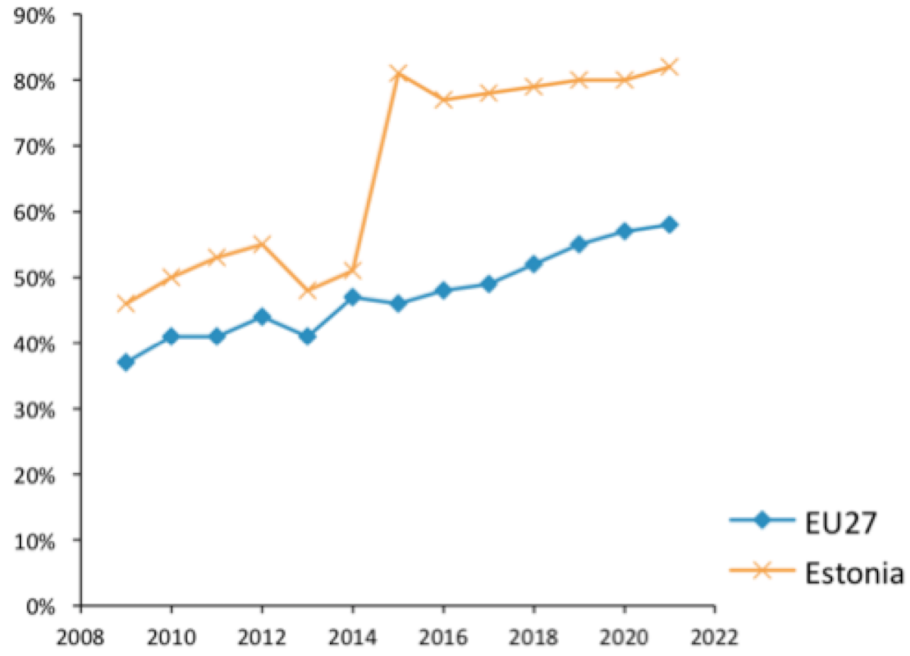
- 70% от естонците използват ежедневно дигиталната си лична карта (2022г.)

- 44% от естонците са избрали да гласуват по интернет на последните парламентарни избори (2019), а 47% на последните избори за Европейски парламент (2019);

Долните графики пък ни разкриват степента на доверие в електронните услуги и употребата им от естонските граждани, в сравнение със средните стойности за Европейския съюз. Данните са от Евростат до 2022 година.

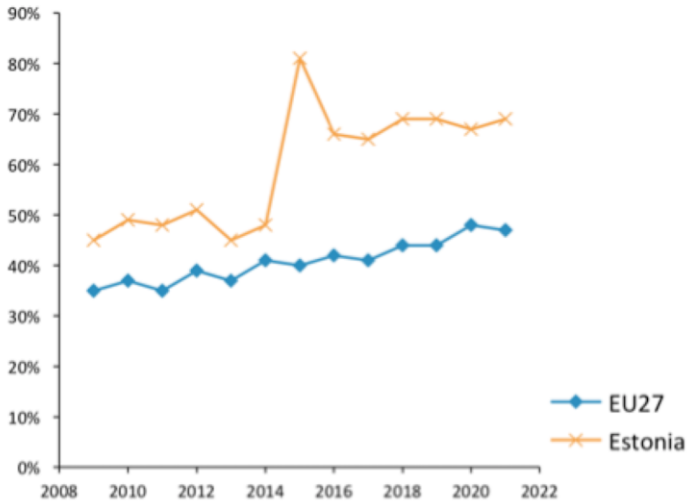
Този документ е създаден по проект „Участие на гражданите в местните политики за осигуряване на киберсигурност за защита на личните данни“, финансиран с административен договор за предоставяне на безвъзмездна финансова помощ BG05SFOP001-2.025-0074-C01/30.08.2022 г., по Оперативна програма „Добро управление” 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

Процент на хората, използващи интернет за взаимодействие с публичните органи в Естония и ЕС



*Източник: Евростат

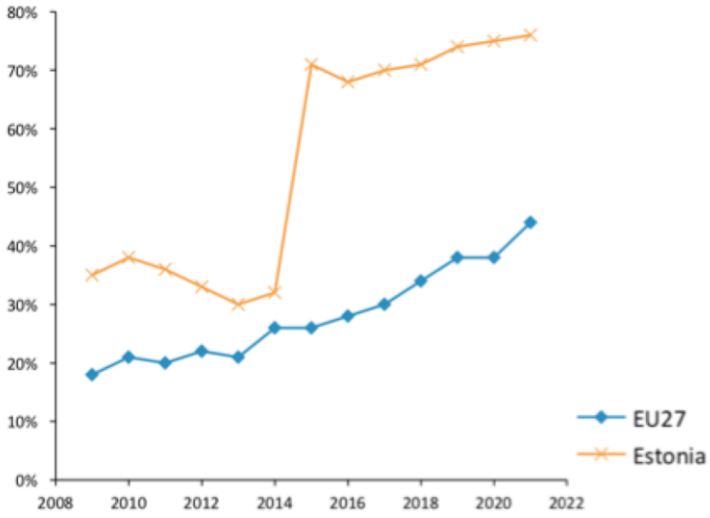
Процент на хората в Естония и средно за ЕС, използващи интернет, за да получат достъп до електронни услуги от правителството



*Източник: Евростат

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

Процент на хората в Естония и средно за ЕС, използващи интернет, за да изпращат попълнени форми до електронното правителство



*Източник: Евростат

Как Естония стигна дотук?

През април 2007 г. естонското правителство решава да премахне паметник от съветската епоха, което предизвиква гневната реакция на властите в Руската Федерация. Чрез диаспората си в страната те инициират протести, които прерастват в кървави бунтове. Дни по-късно Естония се събужда пред лицето на безпрецедентна атака срещу мрежовата си и информационна система. Мнозинството експерти приемат това за първата кибервойна в света.

Разследването показава, че най-малко един милион компютърни устройства са били използвани, в период от три седмици, за атаки срещу уебсайтовете на естонското правителство, банки, медии и редица други частни и публични организации. В пика на тези атаки 58 сайта на правителствени служби са били свалени. Щетите се изчисляват на десетки милиони евро.

Електронните услуги и информационната инфраструктура са били под засилени удари от 27 април до края на месец май 2007 година. Масовите DDoS атаки поразяват ключови правителствени сайтове, които са старателно подбрани, защото са основни елементи от критичната информационна инфраструктура. Хакери фалшифицират сайта на управляващата в Естония партия и пускат “официално” изявление-

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

извинение от името на министър-председателя Андрус Ансип. Постигнат е отказ на достъп до огромен брой електронни устройства: компютри, сървъри, мрежи или интернет ресурси в държавния и частния сектор. Спешният телефон 112 не е бил достъпен за няколко часа на 9 и 10 май. Икономическата дейност в страната е била възпрепятствана по няколко часа на ден заради непрестанни атаки срещу услугите на онлайн банкирането и изпълнението на транзакциите. Засегнати са новинарските порталите на три от шестте основни новинарски организации в страната. Атакувани са рутерите на доставчиците на интернет услуги в страната, с което, на практика, са свалени DNS услугите в малката балтийска държава.

Преди инцидента в Естония от 2007 година кибератаките не са били разглеждани като непосредствена заплаха за националната сигурност на държавите или нейните граждани. Не са били част от стратегическата рамкова сигурност. Дори в контекста на НАТО не са били квалифицирани като атака срещу държава членка, което, респективно, би активирало колективната отбрана съгласно член 5. Случаят “Естония” променя всичко това.

Двата стълба на естонската политика в областта на киберсигурността – Знание и доверие.

Изграждането и поддържането на електронни услуги на публичната администрация не може да се случи без доверие в системата. Националната стратегия за киберсигурност на Естония се развива непрестанно от създаването си през 2008 г., като обхваща целия спектър - от защита на критичната инфраструктура и електронните услуги за гражданите, до повишаване на компетентността в областта на информационната сигурност за цялото общество. Стратегията за киберзащита върви вече 15 години ръка за ръка с друга стратегия от първостепенно значение за държавата, а именно планът, целящ да утвърди Естония като най-устойчивото цифрово общество в Европа.

Анет Нума, съветник по дигитална трансформация от организацията “E-estonia”, разяснява политиката на страната в областта на киберсигурността.

Според Нума има няколко начина, по които Естония може да постигне целите на своята стратегия за киберсигурност и дигитално общество.

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

Правителството трябва да може да се адаптира към промяната, да поддържа и изгражда доверието на гражданите си, да насърчава образованието и киберграмотността и да споделя прозрачно информация, когато това е възможно. Прозрачността и доверието в системата са от първостепенно значение за изграждането на култура в преход към дигитално общество. В тази връзка Нума разкрива, че всеки естонски гражданин може да влезе в портала на електронното правителство и да изтегли списък с държавни институции или дори частни организации, които са разглеждали личната му информация и да изпрати запитване за причините, ако те са му неясни. Освен това, когато страната претърпи киберинцидент или риск за киберсигурността, тя е напълно открита с обществеността относно подробностите и последствията. Пример за това е кризата с личните карти през 2017 г., която накара министър-председателя Юри Ратас да се появи в телевизионно обръщение, за да обясни какво се е случило, как се е случило и как това да не се случи отново.

„Бъдете напълно честни с гражданите и те ще ви се доверят“, казва Анет Нума. „Прозрачност, образование и комуникация. Така караме хората да се доверяват на системата и да използват електронните услуги и продукти“.

Естония се стреми да инвестира в повишаване на дигиталната грамотност на своите граждани още от първия ден, като се отдава огромно значение на цифровите и киберпознания. Това важи както за по-младите, така и за възрастното поколение. Учениците започват обучението си по безопасност на дигиталната сфера още в началното училище и продължават и в средното си образование. Отдава се голямо значение на партньорството между университетите, частния сектор, Министерството на отбраната и Министерството на образованието за повишаване на осведомеността и компетентността на гражданите относно киберзаплахите. Например, през изминалата година естонската компания “Cybexer” обедини усилия с Министерството на отбраната, за да организира обучения по киберсигурност за ученици на възраст до 10 години. Интересът към програмата е бил толкова голям, че списъците са били запълнени за година напред.

В Естония се организира и един от най-известните уъркошопи за експерти по сигурността, защитаващи националните ИТ системи и мрежи. “Locked

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

Shields" се организира ежегодно от "CCD COE" в Талин от 2010 г. насам. Това е най-голямото и най-сложно международно техническо учение и състезание за киберзащита, базирано на сценарии. Всяка година екипите са подложени на натиск да поддържат мрежите и услугите на измислена държава. Това включва обработка и докладване на инциденти, решаване на киберпредизвикателства и реагиране на разнородни сценарии.

За разлика от много други страни, Естония не вярва, че киберзаплахите са просто теоретична опасност. "Всеки месец естонският национален компютърен екип за спешно реагиране регистрира близо 300 киберинцидента. Тези числа представляват събития в киберсигурността, които нарушават поверителността, наличността или целостта на цифровите системи или на данните, съхранявани в тях. А броят на записаните случаи, при които са били предотвратени превантивно щети, включително опити за кибератаки, е повече от три пъти по-голям", цитира данни на агенцията Нума.

"Настоящата киберсигурност на Естония е подкрепена от високофункционална инфраструктура за електронното правителство. От надеждна цифрова мрежа, от задължителна базова линия за сигурност на всички публични органи, както и централна система за наблюдение, докладване и разрешаване на инциденти. Доставчиците на жизненоважни услуги са задължени да оценяват и управляват своите информационни и комуникационни технологични (ИКТ) рискове. Комуникационните мрежи на естонските държавни институции непрекъснато се изследват и картографират и се правят тестови опити за хакване на компютърни мрежи на доставчици на жизненоважни услуги, за да се види и оцени тяхната реакция."

"Най-важното - заключва Анет Нума - е че има консенсус, че киберсигурността може да бъде осигурена само чрез сътрудничество и че е необходим съвместен принос на всички нива – държавно, частен сектор и физически лица".

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

Мерки за киберсигурност, имплементирани в публичната администрация в Естония

Естония е приложила редица мерки за киберсигурност в публичната си администрация за защита от атаки и пробиви на базата данни. Някои примери от столицата Талин включват:

1. Използването на националната система за дигитална лична карта като метод за сигурна онлайн верификация и идентификация посредством електронен подпис;

2. Внедряване на система за своевременно и ефективно реагиране и управление на инциденти по киберсигурността на целия град. Дейността се обезпечава чрез създаването на централизирана система за киберотбрана, известна като Екип за реагиране при спешни компютърни ситуации (CERT);

3. Използването на най-напредничавите техники за криптиране, шифроване и архивиране на чувствителни данни и комуникации;

4. Редовно тестване на сценарии за проникване в мрежите и системите и оценка на уязвимостта за евентуално справяне с потенциални слабости в сигурността;

5. Сътрудничество с частни и правителствени агенции по изготвянето на бюлетин за споделяне на най-добри и актуални практики за подобряване на цялостната позиция на киберсигурността на общинската власт в Талин;

6. Редовно обучение по киберсигурност на служителите в партньорство с частния сектор и университетите;

Анализ на реализираните мерки по киберсигурност в публичната администрация на Естония.

Прилагането на мерки за киберсигурност в публичната администрация на Естония е довело до положителни резултати в борбата със зловредното проникване в системите и мрежите на общинските власти в страната. Важно е да се отбележи, че е трудно да се определи количествено ефективността на резултатите, тъй като много от тях не са измерими, защото голямата част от мерките се въвежда за смекчаване на потенциалните въздействия, тъй като е невъзможно да се гарантира, че

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

няма да възникнат никакви нарушения. Това заключение се отнася за всички държави, които ще бъдат разгледани и анализирани в този доклад. Също така е важно да се акцентира, че пейзажът на заплахите непрекъснато се развива и усложнява, като постоянно се появяват нови вируси или методи за компрометиране и кражба на чувствителни данни. Ето защо ефективността на мерките за киберсигурност трябва непрекъснато да се оценява и актуализира, за да се гарантира, че те остават ефективни пред лицето на новите опасности в Мрежата.

Може би най-важният качествен измерител за адекватността и надеждността на мерките и политиките срещу киберпрестъпността в публичната администрация на Естония е нарастващото доверие от гражданите в електронното правителство и услугите, които то осъществява и предлага. Естонското правителство декларира, че в резултат на предприетите мерки кибератаките с мащабно въздействие върху електронните услуги и останалата критична инфраструктура са намалели чувствително.

Използването на усъвършенствани техники за криптиране и редовни тестове за проникване и оценки на уязвимостта са помогнали да се идентифицират и адресират потенциални слабости в сигурността, намалявайки по този начин риска от успешни кибератаки. Внедряването на системи за управление на инциденти пък е спомогнало за откриването и реагирането на киберпробиви в много по-кратки срокове, което е важно за намаляване на цялостното въздействие на инцидента върху данните и мрежата.

В заключение, макар да е трудно да се представят конкретни количествени измерители, за да се демонстрира намаляването на киберзаплахите в естонската публична администрация в резултат на прилагането на мерки за защита на киберсигурността, експерти по сигурността потвърждават, че Естония разполага с една от най-стабилните и напредичави инфраструктури за киберсигурност в Европа.

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

Германия

Обновеният закон за ИТ сигурността на Германия следва примера на актуализираната Директива на ЕС за мрежова и информационна сигурност (МИС2). Политиката на Федералното правителство определя новите изисквания за сигурност, като добавя и структурите на общинската власт към списъка от организации, опериращи в сферата на критичната инфраструктура. Те имат срок до 1 май 2023 година, за да влязат в крак с новите технически и оперативни изисквания. Повишават се правомощията на Федералната служба за информационна сигурност (BSI) да координира изпълнението на мерките, заложени в стратегията.

Новите политики и приоритети на Федералната република, отнасящи се и за информационните и мрежови системи и база данни на публичната администрация, включват:

1. Организациите, имащи статут на такива със "специален обществен интерес", са задължени да внедрят техническа и оперативна система за ранно засичане на киберзаплахи и уязвимости най-късно до 1 май 2023 г. От технологична гледна точка трябва да се внедрят следните модули за ранно засичане на заплахи срещу критичната инфраструктура и срещу базата данни от чувствителна и поверителна информация.

а. Система за анализ на регистрационни данни, известен също като управление на информация за сигурността и събития;

б. Vulnerability Management & Compliance система за цялостно сканиране на уязвимости и съвместимост;

в. Система за анализ на поведението на мрежата за оценка на потоците от данни и свързаната с тях информация;

г. Система за откриване и реакция при крайните точки, която се използва за индикация на свързани със сигурността събития с различна степен на критичност;

2. Организациите, имащи статут на такива със "специален обществен интерес", са задължени да уведомяват Федералното министерство на вътрешните работи на Германия и Федералната служба за информационна сигурност при закупуването и внедряването в оперативния си процес на

технически и софтуерни компоненти, които ще взаимодействат с елементи от системата на критичната инфраструктура. Например, ако производителят е контролиран от трета страна или противоречи на целите на политиката за сигурност на германското федерално правителство, ЕС или НАТО.

3. Организациите, имащи статут на такива със "специален обществен интерес", ще бъдат обект на регулярен одит и сертификации, за да покажат как са защитени техните системи и как е повишена компетентността на служителите им в сферата на киберсигурността.

Макар темата за информационната сигурност в местното самоуправление на Германия да е сравнително нова и да липсва обемно количество изследвания в областта, по-долу ще обърнем внимание на едно такова. Дело е на преподаватели от института за Компютърни науки към университета в Росток. Те правят сравнителен анализ на 48 малки и средни предприятия с местната администрация в провинциите Заарланд и Бавария. Целта на изследването е да разпише основните политики, които опосредстват създаването и управлението на една ефективна среда, защитена от зловредните въздействия в сферата на киберсигурността.

1. Лидерство - Лидерската инициатива и задаването на пример от най-високото ниво в управленската йерархия е основната предпоставка за успешното създаване и прилагане на стратегията за информационна и мрежова сигурност в една организация или общинска власт;

2. Организационна структура - Планирането и изпълнението на процеса на сигурност включва дефинирането на организационната структура и точното разпределение на ролите и задачите;

3. Организация на процеса – Всяка една организация, в това число и публичната администрация, има богат и разнообразен набор от задачи, приоритети и отговорности. Необходимо е тези, свързани със сигурността на информационната и мрежова система, да не бъдат "разхвърляни" и "раздробявани" по места, а да бъдат организирани в самостоятелен сбор от процеси, които да имат конкретен "собственик" на процеса, т.нар. отговорно лице;

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. Информираност на служителите – 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, е от ключово значение за изграждането на една цялостна среда на сигурност в структурите на местната власт;

Успешен пример за имплементирането на силни и ефективни мерки в сферата на киберсигурността на местно ниво е град Франкфурт. Там е създадено звено за киберсигурност (CSU), което наблюдава, анализира и оценява оперативната и техническа способност на администрацията за справяне с предизвикателствата на киберпрестъпността. Звеното има за задача да гарантира и контролира, че всички мрежови и информационни системи, както и масиви от данни, са достатъчно добре защитени. CSU работи в тясно сътрудничество с ИТ отдела на градската власт за прилагане на мерки като, например, двуфакторно удостоверяване на акаунтите, криптирането на данни и изграждането на “защитни стени”. CSU съблюдава още за редовна промяна на паролите с цел предотвратяване на неоторизиран достъп до акаунтите. Важна задача на CSU е не просто да оказва техническа помощ в имплементирането на мерките, а да “приобщи” всички служители към съответствие с новите политики. CSU провежда редовни обучителни сесии по добри практики, за да повиши осведомеността на служителите относно важността на киберсигурността и ролята, която всеки един от тях играе в процеса на защитата на системите на общината.

Резултатите от усилията на GSU са оценени като изключително положителни и ефективни, довели до чувствително намаляване на случаи на “небрежност” и “немарливост” от страна на служителите, водещи до неоторизиран достъп до техните пароли и акаунти.

Друга общинска власт, която е въвела сходни мерки за киберсигурност, е Хамбург. ИТ отделът на общината работи в тясно сътрудничество с външни експерти по киберзащита от частния ИТ сектор в прилагането на редица напредничави технически мерки. В допълнение, местната власт в Хамбург

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

има ежегодни програми за обучение и сертификация на служителите си за това как да идентифицират и да се пазят от потенциални кибератаки.

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. За да се справи с това, Хамбург кандидатства за финансиране чрез безвъзмездни средства на европейско и федерално ниво, както и чрез сключването на партньорства с външни организации от частния сектор.

Освен техническите мерки и такива, свързани с обучението на служителите, за общините е важно още да разполагат с план в случай на пробив в киберсигурността. Такъв има градската управа на Берлин, създаден в кооперация с външни експерти на федерално ниво и такива от частния ИТ сектор. Берлин разполага с цялостен план за реагиране при инциденти в сферата на киберсигурността, който очертава стъпките и сроковете, които трябва да се предприемат в случай на пробив. Това включва оценка на инцидента, ограничаване на въздействието, ликвидиране на последствията от заплахата и възстановяване целостта на данните и мрежата.

Киберсигурността е от първостепенно значение за общините в Германия, които оперират с елементи от критичната инфраструктура на страната. Чрез внедряването на силни политики и протоколи като: двуфакторно удостоверяване, криптиране на данни, редовни промени на пароли, и инвестирането в обучение и сертифициране на служителите общините могат ефективно да защитят себе си и своите системи от киберзаплахи. В случай на инцидент наличието и задействането на план за реакция също е от решаващо значение за минимизирането на въздействието от кибератака. Важно е да се отбележи, че е трудно да се определи количествено ефективността на резултатите. От една страна, защото мнозинството мерки са имплементирани сравнително скоро, а от друга страна, тъй като много от тях не са измерими, защото голямата част от мерките се въвеждат за смекчаване на потенциалните въздействия, тъй като е невъзможно да се гарантира, че няма да възникнат никакви

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

нарушения. Това заключение се отнася за всички държави, които ще бъдат разгледани и анализирани в този доклад.

Франция

В националната стратегия по киберзащита на френското правителство са заложени редица политики и мерки по обезпечаване сигурността на информационните мрежи, системи и база данни, поддържащи електронните услуги на публичната администрация. Стратегията определя цялостния подход на властите към заплахите в киберпространството и очертава основните цели и действия, които трябва да бъдат предприети за защита на критичната инфраструктура на страната и цифровия суверенитет. Агенцията, която отговаря за координирането и прилагането на набелязаните цели и политики, е Националната агенция за киберсигурност (ANSSI) на Франция.

Само в периода 2015-2020 няколко главни френски града са били обект на сериозна кибератака. През 2015 г. Лил е засегнат от атака със "зловреден софтуер" (ransomware), който блокира компютърните системи, причинявайки прекъсване на услуги като обществения транспорт и административните дейности на кметството.

През 2020 г. градовете Ница и Вилеюф също са засегнати от атака с ransomware, която довежда до временно спиране на компютърните системи, а на местната власт се е наложило да плати откуп в неназован размер, за да си възвърне достъпа до файловете и паролите. Кибератаките срещу публичната администрация стават все по-често явление и представляват заплаха за националната сигурност на страната.

В съответствие с имплементирането на директивата за Мрежова и информационна сигурност (МИС2) и добавянето на структурите на местната власт към списъка от организации, за които ще се прилагат разпоредбите, Сенатът на Франция одобри конкретна програма за привеждане на публичната администрация в съответствие. Тя включва:

1. Програма за информираност на служителите. Изследване от 2021 година сред малките и средни общини във Франция показва високият процент дивиация и неравномерност в разбирането и информираността за рисковете в киберпространството спрямо по-големите общини. В по-

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

малките общини проблемът все още се възприема като чисто технически, който трябва да включва единствено определени лица със специализирани умения. При по-малките общини въпросите на киберсигурността все още се подценяват и в тях липсва разбирането за необходимостта от интегриран подход с междуфункционална визия за решаване на проблемите. В тази връзка Сенатът цели да намали несъответствията между големите и малки общини по въпроса с осведомеността. В плана е заложено създаването на платформа с видеосъдържание, целящо да информира служителите относно рисковете в киберпространството и съвети за защита - управление на пароли; как да различаваме фишинг и рансъмуер; видеоматериали, описващи първите стъпки, които трябва да се предприемат в случай на кибератака; как да се извърши бърза самодиагностика в случай на инцидент; практически ръководства по киберсигурност и други.

2. Курсове по киберсигурност за публичната администрация като част от Плана за възстановяване на ЕС. Френското правителство е определило 136 милиона евро за периода 2021-2022, които да се инвестират в „компонент за киберсигурност“, ръководен от Националната агенция за сигурност на информационните системи (ANSSI) и насочен към служителите на местните власти.

3. Регионални центрове за реагиране при киберинциденти. ANSSI подкрепя седем региона на Франция в създаването на центрове за реагиране при киберинциденти. Тези Екипи за реагиране при инциденти с компютърната сигурност (CISRTs) ще отговарят за обучението и повишаването на осведомеността на местните власти. Паралелно с това те ще подпомагат публичната администрация в докладването на киберинциденти. Експертите от CISRTs ще съветват потърпевшите в това как да квалифицират инцидентите и как да се свържат с най-подходящите структури, които да им помогнат при разрешаването на проблемите.

4. Схема за подпомагане на придобиването и внедряването на продукти и услуги в сферата на киберсигурността в общините. Целта на новосъздадената схема е да подпомогне местните власти в придобиването на софтуер и хардуер, необходим за дигиталната им трансформация и киберзащита. Тези продукти и услуги трябва да засилят нивото 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

киберсигурност на структурните бенефициенти и в съответствие с техните непосредствени и индивидуални нужди.

5. Сенатът насърчава обединяването на ресурси на общинско или департаментско/регионално ниво. Сенатът препоръчва обединяването на ресурси между "малките" и големите", което да даде възможност на малките местни власти да се справят с недостига на квалифицирани специалисти.

Мерките за защита на информационните и мрежови системи, имплементирани на общинско ниво във Франция, са сходни навред и са подчинени на политиките за сигурност, залегнали в регулаторните и стратегически императиви на френското правителство в сферата на киберсигурността. Въведените мерки целят да защитят критично важните цифрови системи и инфраструктура на френската държавна и местна администрация.

Градовете Лион и Тулуза, например, са създали собствени звена за киберсигурност, за да защитят своите цифрови системи и инфраструктура. Това звено е отговорно за наблюдението и реагирането на кибернетични заплахи, както и за прилагането на мерки за сигурност като редовни актуализации на сигурността, откриване и предотвратяване на проникване и планове за реакция при инциденти. Те също имат специализиран екип за бързо реагиране.

Примери за конкретни имплементирани мерки в сферата на сигурността включват:

1. "Защитни стени" за протекция срещу неоторизиран достъп до мрежите и системите чрез контролиране на входящия и изходящия трафик. Те могат да бъдат конфигурирани да блокират определени видове трафик като, например, входящ трафик от известни злонамерени IP адреси.

2. Системи за откриване и предотвратяване на проникване (IDPS), които също се използват за откриване и предотвратяване на неоторизиран достъп до мрежи и системи. Те могат да бъдат конфигурирани да предупреждават администраторите за подозрителна дейност, като неуспешни опити за влизане или опити за достъп до ограничени зони на мрежа.

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

3. Шифроване и криптиране, което се използва за защита на чувствителни данни като лична информация и финансови транзакции от неоторизиран достъп. Това може да се приложи за данни в покой или в транзит като, например, за имейл или мрежов трафик.

4. "Контрол на достъпа" са набор от мерки, които се използват, за да се гарантират, че само оторизирани потребители имат достъп до чувствителна информация и системи. Това може да включва мерки като удостоверяване на потребителя, ролеви контроли за достъп и разрешение за сигурност за определени нива на достъп.

5. Актуализации на защитата и правенето на корекции при нужда. Редовното актуализиране на софтуер и системи с корекции за сигурност е жизненоважна мярка за поддържане на мрежите и системите защитени. Това помага да се коригират известни уязвимости, които могат да бъдат използвани от нападателите.

6. Реагиране при инциденти и планове за възстановяване. Френските общини като Лион и Тулуза разполагат с планове за реагиране при инциденти и възстановяване, за да се справят с евентуална кибератака и за да сведат до минимум щетите, като възстановят функционирането си максимално бързо. Това включва наличието на специален екип за реагиране при инциденти, който отговаря за справянето с киберинциденти и осигуряването на непрекъснатост на операциите.

7. Редовни одити и оценки на сигурността. Френските общини провеждат редовни одити и оценки на сигурността, за да идентифицират уязвимостите в своите мрежи и системи. Това може да включва сканиране на "слаби точки", тестове за проникване и оценки на сигурността на трети страни доставчици и партньори.

8. Обучение на служителите. Обучението на служителите е от съществено значение за създаването на култура на осъзнаване на сигурността. Много френски общини са въвели редовни програми за квалификация, за да обучат служителите си относно най-добрите практики в киберсигурността и как да не станат жертва на атаки чрез социално инженерство.

Всички гореспоменати мерки са предназначени да работят заедно, за да осигурят цялостна защита срещу киберзаплахи и да сведат до минимум

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

въздействието на всякакви успешни атаки. Макар да е рано за задълбочено количествено и качествено измерване за ефективността на мерките, френските експерти в сферата на киберсигурността поощряват правителството и общинските власти за предприемането на конкретни стъпки за защитата на критичната информационна и системна инфраструктура на публичната администрация. Експерти потвърждават, че в резултат на повишаване квалификацията и компетентността на служителите във френските общински власти относно заплахите в киберпространството, са намалели чувствително случаите на пробив на акаунти и пароли от "немарливост" и "неглижиране", а това е един от най-честите способи на хакерите да компрометират или откраднат чувствителна информация.

Италия

През май 2022 година Италия представи първата си национална стратегия за киберсигурност. Заложено в нея е страната да отделя 1,2% годишно от брутните си национални инвестиции за подобряване на киберсигурността. Приоритет и акцент в стратегията се поставя и върху структурите на общинската власт.

„Италия иска да постигне стратегическа автономия и цифров суверенитет, като създаде и отглежда една екосистема за киберсигурност, основана на публично-частно партньорство", казва министър-председателят Марио Драги по време на презентацията.

Документът идентифицира три приоритетни области на действие:

1. Превантивност на престъпната дейност в киберпространството. Ограничаване на въздействието от зловредни инциденти, дело на киберпрестъпници, хакерски активисти или координирани държавни кампании, които използват слабости в мрежовите и системни протоколи, за да откраднат данни или да повредят компютърната екосистема. За пример са дадени DDoS инцидентите, чрез които руските хакерски колективи като "Killnet" и "Legion" атакуват италианските публични институции.

2. Дигитална устойчивост на публичната администрация, технологичната ѝ обезпеченост и защитата на чувствителните информационни и мрежови системи.

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

3. Борба с онлайн дезинформацията. Включва превенция на разпространяването на фалшиви новини, дезинформационни кампании, които объркват, настройват и дестабилизират гражданското общество. Правителството се надява да противодейства на фалшивите новини със „синергични превантивни и правоприлагащи действия“, за да „осуети опитите за подкопаване на ценностната система“, на която се основава страната.

Както се вижда, защитата на италианската публична администрация от зловредните дейности в киберпространството е един от трите колони на стратегическата рамка за сигурност. Тя включва следните конкретни политики и приоритети:

1. Укрепване на способностите за разузнаване, правоприлагане и превантивна отбрана на елементите на критичната инфраструктура и информационната база данни от значение за националната сигурност;

2. Подпомагане на индустриалното и технологично развитие. Подобряване на технологичните, оперативните и аналитичните способности за киберзащита на публичната администрация и останалите организации от критичната инфраструктура;

3. Насърчаване на публично-частното сътрудничество в сферата на киберзащитата;

4. Насърчаване на култура на осведоменост сред служителите в областта на киберсигурността;

5. Подпомагане на международното сътрудничество, обмяна на опит и киберучения;

6. Актуализиране на законодателството за киберсигурност в съответствие с международните стандарти на ниво ЕС и НАТО;

7. Изготвянето на нови Протоколи за сигурност и действие при кризи в съответствие със стандартите на ЕС и НАТО;

Италианското правителство работи активно за подобряване на киберсигурността на своята мрежа и информационни системи. Министерството на икономическото развитие отговаря за координирането

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 прилагането на политиките за киберсигурност в Италия. Важно е да се отбележи още, че италианското правителство създава агенция за киберсигурност, която отговаря за предоставянето на насоки и подкрепа на организациите и публичната администрация по въпросите на киберсигурността. Тя също координира с други национални и международни органи инициативи за споделяне на информация за киберзаплахи и най-добри практики за защита.

Агенцията за киберсигурност издава минималните мерки за сигурност на информационните и мрежови системи, които имат за цел да противодействат на най-честите киберзаплахи в италианската публична администрация. Мерките се състоят в технологичен, организационен и процедурен контрол:

Технически мерки:

1. Сегментиране на мрежата: Мрежите на публичната администрация трябва да бъдат сегментирани, за да се предотврати разпространението на кибератака в чувствителни зони на мрежата до цялата система;

2. Защитни стени и системи за откриване/предотвратяване на проникване (IDS/IPS). Тези методи се използват за наблюдение на мрежовия трафик и откриване и предотвратяване на неоторизиран достъп или злонамерена дейност;

3. Криптиране. Системите и файловете на публичната администрация са криптирани, за да се предпазят от неоторизиран достъп или разкриване;

4. Управление на уязвимости. Организациите на публичната администрация редовно сканират своите системи и мрежи за уязвимости и след това прилагат корекции и актуализации, за да ги адресират;

5. Двуфакторно удостоверяване. От служителите на публичната администрация се изисква да използват двуфакторно удостоверяване за достъп до чувствителни системи и данни;

Оперативни мерки:

1. Управление на инциденти в киберсигурността. Организациите на публичната администрация трябва да разполагат с разписани планове,

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

отговорни лица и срокове за реакция при инциденти и екипи за управление на инциденти, за да реагират бързо и ефективно на киберинциденти;

2. Обучение по киберсигурност. Служителите в публичната администрация трябва редовно да преминават обучение по киберсигурност, за да са в крак с най-актуалните рискове и методи за защита в киберпространството;

3. Съответствие. От публичните административни организации се изисква да спазват разпоредбите и законите като Общия регламент за защита на данните (GDPR) и Кодекса за цифрова администрация за защита на личните данни и държавните активи;

4. Редовни оценки на сигурността. От организациите на публичната администрация се изисква редовно да оценяват състоянието си на киберсигурност и да прилагат необходимите мерки за подобряването ѝ;

5. Приемане на международни стандарти и най-добри практики за киберсигурност като, например, стандарта ISO/IEC 27001;

Макар с различен темп, италианските общински власти имплементират или вече са имплементирали основната част от мерките. Предизвикателствата пред тях са в задължителния характер, който тези мерки започват да имат с въвеждането в действие на новата стратегия за киберсигурност на организациите от "критичната инфраструктура". По-малките общини ще трябва тепърва да кандидатстват за бюджетни ресурси, за да въвеждат изискванията за сигурност и защита. Не по-малко предизвикателство е и създаването и поддържането на ИТ звена от специалисти в по-малките общински структури.

В тази връзка е трудно за момента да се оцени задълбочено ефективността на мерките за киберсигурност в публичната администрация на Италия. Важно е да се отбележи, че е невъзможно напълно да се предотвратят кибератаките, като целта е да се минимизират щетите, причинени от тяхното въздействие, и да се предприемат мерки за бързото възстановяване на мрежите и процесите. Затова и в количествено отношение не винаги броят увеличени или намалени киберинциденти разкриват цялата същност на проблема. Също е важно да се отбележи, че внедряването на мерки за киберсигурност е непрекъснат процес, тъй като непрекъснато възникват нови заплахи и уязвимости, все по-комплексни 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

целенасочени, и организациите трябва да адаптират своите мерки за сигурност, за да изпреварят заплахите.

В заключение, въпреки че е трудно да се определи ефективността на мерките за киберсигурност в италианската публична администрация без конкретни данни, е видно, че правителството предприема активни стъпки за подобряване на киберсигурността, като предоставя ресурси и стратегии за подкрепа, за да помогне на организациите да подобрят своето състояние на киберсигурност.

Испания

Според GCI (Глобален индекс на киберсигурността), публикуван от ITU (Международен съюз по телекомуникации), Испания е 4-та европейска държава и 7-ма в света по отношение на технологичното и оперативно ниво на зрялост на своята киберсигурност. Страната има и своя град - шампион в областта на киберзащитата. Леон е испанската столица на киберсигурността. Не само защото е седалището на Националния институт по киберсигурност на страната, но и защото демонстрира способността си да създава успешно технологични, бизнес и изследователски синергии, от които се възползват не само структурите на местната власт, но и много по-широк набор от организации в публичния и частен сектор.

Подходът на Испания за справяне с предизвикателствата и заплахите на киберпрестъпността в държавната администрация е с акцент върху публично-частното партньорство, чрез което се черпи експертизата и опита на ИТ индустрията.

В края на ноември 2022 година Националният криптологичен център на Испания (CCN-CERT) подписва рамков договор за сътрудничество с компанията експерт в сферата на киберсигурността - “Crossword” - за внедряване в публичната администрация на системата “Trillion”, която да осигури холистична защита на компютърните и информационни мрежи. “Trillion” е автоматизирана, облачно-базирана платформа за анализ и сигнализация на уязвими и потенциално уязвими акаунти. Информацията се генерира и получава ежедневно в централизирано, специализирано звено на испанския криптологичен център, който анализира резултатите и прави препоръки за отстраняване на засечените уязвимости или пропуски.

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

Предисторията на това сътрудничество е от 2020 г, когато по време на разгара на пандемията от Covid-19, CCN-CERT действа решително, за да подобри сигурността на испанската здравна инфраструктура. След период на успешна работа в сектора на здравеопазването, CCN-CERT решава, че разширяването на обхвата на "Trillion" до цялата публична администрация ще осигури по-надеждна защита на мрежовата и цифрова система, на електронните услуги, както и на потребителските акаунти и пароли.

Основен акцент в Националната стратегия за киберсигурност на Испания е да образова широката общественост относно заплахите в мрежовата и информационна среда. Повече от 70% от населението на Испания използва интернет/дигитални услуги на ежедневна база (испанска статистическа служба, 2021) и властите осъзнават, че единственият начин да се сведе броят на инцидентите свързани с пробив на акаунти и пароли, е да се инвестира в образователни кампании. Когато става въпрос за обучение по киберсигурност и налични програми и ресурси за това, Испания превъзхожда много други европейски страни. Конкретни данни за 2017 г. показват, че Националната полиция на Испания в сътрудничество с местната власт и централните органи по киберсигурност е организирала общо 56 715 дейности по превенция на киберзаплахите. Това включва срещи, беседи, лекции, обучения, медийни кампании и други дейности.

В продължение на две години, от 2017 до 2019, Автономният университет на Мадрид ръководи проект, финансиран от ЕС, насочен към укрепване на публично-частното сътрудничество в борбата с киберпрестъпността. По-специално, той се стреми да свърже общинската власт, академичните среди, местните образователни органи и частните компании чрез създаването на инкубатор и център за върхови постижения в сферата на киберсигурността, от който да черпят познание и ресурси всички заинтересовани страни.

Градската власт на Мадрид пък показва отговорен подход към по-малките общини, като по собствена инициатива създава програма и инвестира ресурс, за да осигури покритие за киберсигурността на малките местни администрации. По този начин градските власти показват нагледно, че битката с киберпрестъпността действително трябва да бъде холистичен процес, в който не бива да бъдат неглижирани "малките", чрез създаване на неравномерности и слаби звена, защото те могат да уязвят цялата система.

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

Мадрид планира да създаде и финансира агенция, която ще отговори на нуждите на градските съвети по отношение на превенцията и реакцията на атаките в киберпространството. Това е анонсирано в края на октомври 2022 от общинския съветник по цифровизацията, Карлос Искиердо.

„Ние ще отговорим на всички тези нужди със създаването на Агенция за киберсигурност. Този бъдещ орган ще действа в местни единици с по-малко от 20 000 жители, които нямат стратегии или средства за защита на своите мрежи и системи. Този проект ще послужи като ръководство за насърчаване и консолидиране на иновациите на цялата територия, достигайки 100% от администрациите, компаниите и всички граждани в метрополията на Мадрид“, казва депутатът.

Испанските общински структури са имплементирали всички базови технологични и оперативни мерки, които вече бяха разгледани в предходните примери. Затова, вместо да ги преповтаряме, тук ще поставим акцент върху един изключително напредничав и отговорен подход, който би послужил като добър пример за всички останали европейски общински структури. А именно, богата и развита община като Мадрид да поеме доброволно диригентската палка, като инвестира собствен ресурс, финансов и кадрови, за да подпомогне по-малките общини в разработването на стратегия срещу киберпрестъпността и имплементирането на конкретни технически и оперативни мерки за защита. Това показва едно много високо ниво на осъзнатост от отговорните лица в общинската комисия по дигитализация на Мадрид, че в битката с кибератаките никой не може да бъде самостоятелен остров и че цялостната ефективна сигурност на мрежата се оценява по степента на достатъчна защитеност на най-слабите звена в нея.

Рано е да се анализират резултатите от подобен подход към киберсигурността на общинските структури в Испания, но с голяма доза увереност можем да заключим, че трансферът на знания, умения, опит и ресурси ще транспонира в една по-ефективна защита на цялата мрежа на публичната администрация в страната.

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

Нидерландия

Нидерландската полиция докладва, че макар всички останали видове престъпления в страната да бележат спад през 2022 година спрямо 2021, киберкриминалността се е увеличила притеснително в сравнение с нивата от 2019. Броят на докладваните случаи е нарастнал от 4 715 сигнала през 2019 г. до 13 949 през 2022 или иначе казано, инцидентите, свързани с кибератаки са нараснали почти три пъти от нивата си преди пандемията.

Предизвикателството за подсигуряването на целия домейн на сигурността в кибернетичното пространство е твърде голямо за една организация, агенция или дори цяло правителство да се справят сами. Затова основният акцент на нидерландската стратегия за борба с киберпрестъпността е в публично-частното партньорство.

Взаимодействие в изграждането на синергии, организирано на доброволно, равнопоставено и прозрачно участие на всички страни, които имат отношение по въпроса, както и експертизата да помогнат в решаването на проблемите на сигурността на публичната администрация и частния сектор. Целта на нидерландското правителство е да стимулира засилването на сътрудничеството между публичните органи и бизнес общността, чрез създаване на национална мрежа от партньорства за киберсигурност, където големите компании ще подкрепят малките фирми, както и структурите на местната власт в повишаване на знанията им за превенция на инциденти в сферата на киберсигурността.

През декември 2022 г. страната актуализира и представи своята нова стратегия за киберсигурност (2022-2028), в която правителството следва широкообхватен, национален план за укрепване на публичните и частни мрежови и информационни системи срещу нарастващия киберриск в страната. Нидерландският национален център за киберсигурност възприема главна роля в имплементирането на тази стратегия. Агенцията ще има решаваща роля в координирането на плана, изпълнението на мерките и насърчаването към участие в публично-частни партньорства с цел подобряване на киберсигурността.

По-рано тази година оценката на киберсигурността на Нидерландия 2022 (CSAN 2022) установи, че дигиталната защита на страната и в частност тази

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

на публичната администрация не е в крак с иновативността и комплексността на атаките, които непрестанно еволюират и заплашват националната сигурност на страната.

По тази причина е въведен съгласуван пакет от мерки за подобряване на сигурността на електронното правителство по отношение на критичната цифрова инфраструктура и база данни, както и допълнително стандартизиране и хармонизиране на нормативните разпоредби за информационна сигурност. Това включва създаването и прилагането на базова линия за сигурност на чувствителната информация на всички структури на държавната и общинска власт. Заложените в стратегията мерки, също така, целят намаляване на административната тежест за общините в областта на информационната сигурност, включително групирането на одити и оценки в една цялостна верига на отчетност. Правителството се ангажира още и със създаването на съюз за киберсигурност, който да гарантира, че публичните и частните страни прилагат мерките от националния дневен ред равнопоставено и не създават “дупки” в сигурността на цялата система.

Актуализираната стратегия за киберсигурност начертава за нидерландските общини задължителните политики за имплементиране на мерки в сферата на киберсигурността.

1. Обучение и повишаване степента на осведоменост. Повечето пробиви в сигурността при боравенето с компютърни системи и предоставянето на електронни услуги като изтичане на данни, пароли, системни хакове са причинени от т.нар. „човешки елемент“. Обобщено, така наричаме “немарливото” отношение към протоколите за сигурност – забравени или изгубени флашки, съдържащи поверителна информация; кликване върху връзки в имейли от ненадежден източник; създаване на лесна парола, както и такава, използвана в множествени акаунти. Планът изисква от общинските власти да се организират обучения за осведоменост относно рисковете и заплахите за киберсигурността, както и за начините грешките, пораждащи инцидентите, да бъдат сведени до минимум. Препоръчва се това да става чрез партньорство с външни обучители и експерти от сферата на киберсигурността.

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

2. Базови технически мерки. Като задължителен минимум стратегията изисква от ИТ отдела на публичната администрация да въведе протоколи за инсталиране на нов софтуер, които да сертифицират, че преносимите носители на данни (като USB устройства, например) се тестват автоматично за вируси и зловреден софтуер, преди да бъдат използвани. Също така се изисква инсталирането на "защитна стена"; използването на актуален и постоянно актуализирван антивирусен софтуер; въвеждането на двуфакторно удостоверяване за достъп до бизнес системите и акаунтите; въвеждане на система за архивиране на базата данни, за предпочитане чрез "облачни" услуги.

3. План за реакция при инцидент и редовен одит на системите и протоколите за киберсигурност. От публичната администрация се изисква да въведе в съответствие с най-високите стандарти и съвети, предоставени от експертите, план за реакция при настъпването на инцидент и пробив в киберсигурността. Това включва кризисен протокол, който да показва стъпките, които трябва да се предприемат за докладване на инцидента и минимизиране на неговото въздействие, както и да разписва ролите, отговорностите, задълженията и сроковете, които трябва да се спазят. Стратегията също така изисква от общинските власти да въведат постоянен вътрешен и външен одит на системите за киберсигурност от оторизиран източник, за да се набележат превантивно уязвимостите в системата и да се отстранят.

Нидерландия следва своята дългогодишна политика на индивидуалистично, либерално, но отговорно поведение, което прехвърля и на служителите в общинските власти по отношение на киберсигурността. Имплементирането на мерки за дисциплинирано, информирано и осведомено решение на проблема с "немарливостта" и "неглижирането" на протоколите по сигурността е довела до значителен спад на случаите на откраднати данни и пароли. В допълнение, насърчаването на сътрудничество между местните власти и частния сектор в разработването и въвеждането в употреба на продукти и услуги в сферата на киберсигурността е довело до положително справяне с най-често срещаните форми на социално инженерство в дигиталната среда.

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

Може да се каже все пак, че е трудно да се оцени напълно обективно ефективността на мерките, заложени в политиките и стратегията на местните власти за борба с киберпрестъпността. Това е така, защото ефективността на подобни мерки често се определя по това дали евентуална кибератака е щяла да се състои, ако не са били налични определени защитни способи за задържане. Подобни случаи обаче значително по-трудно се докладват, тъй като често протичат, без да оставят конкретен маркер в системата за сигурност.

Все пак експертите в областта на киберсигурността са категорични, че прилагането на синхронизирани и цялостни мерки за превенция на най-често срещаните видове киберинциденти има значително въздействие както количествено, така и качествено върху сигурността на мрежата и информационните системи. Те предпазват от широк набор от киберзаплахи, включително вируси, зловреден софтуер, фишинг атаки и неоторизиран достъп до чувствителни данни.

Швеция

Скандинавската държава има национална стратегия за киберсигурност, която приоритизира защитата на критичната инфраструктура; разработването на способности за откриване, предотвратяване и реагиране на кибератаки срещу правителствените и общински мрежови и информационни системи; подобряване на способността за бързо и ефективно реагиране на киберинциденти и минимизиране на причинените щети от киберзаплахи; насърчаване на осведомеността и образованието относно киберсигурността сред публичния и частния сектор.

Шведската агенция за непредвидени ситуации (MSB) отговаря за координирането на усилията по изпълнението на плана и стратегията на страната в сферата на киберсигурността и работи в тясно сътрудничество с други правителствени агенции като, например, шведските Въоръжени сили и шведската Национална полиция, а също и с организации от частния сектор и международни партньори.

Защитата на мрежовата и информационна система на шведското електронно правителство както на държавно, така и на общинско ниво е основен стълб и приоритет в цялостната стратегия на скандинавската

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

държава да противостои на заплахите в кибернетичното пространство. Политиките и имплементираните мерки в тази сфера не са по-различни от онези, приложени в останалите разглеждани европейски държави, и включват:

1. Управление на риска. Общинските власти в сътрудничество с оторизирани правителствени агенции или външни фирми провеждат редовни оценки на риска, за да идентифицират потенциални уязвимости и заплахи за своите системи и услуги. Въз основа на тези оценки се прилагат подходящи мерки за смекчаване или елиминиране на идентифицираните рискове.

2. Мрежова сигурност. Общинските власти са въвели конкретни мерки за мрежова сигурност, за да защитят своите компютърни системи. Това включва имплементирането на силни методи за удостоверяване на достъпа до правителствени/общински акаунти и електронни услуги (многофакторно удостоверяване); редовни актуализации на сигурността; внедряване на системи за идентифициране и предотвратяване на проникване; използването на защитни стени, виртуални частни мрежи (VPN)

3. План за реакция при инциденти. Общинските власти разполагат с кризисен план за реагиране при инциденти. Той включва процедури за идентифициране и ограничаване на случаи на пробив в системите и базата данни. Разписва ролите, отговорностите и сроковете за действие, както и включва процедури за възстановяване на жизненоважните операции в следствие на инцидент.

4. Обучение и повишаване на осведомеността. Общинските власти в сътрудничество с академичните среди и ИТ експерти организират редовни програми за обучение и осведомителни кампании за своите служители. Това помага да се гарантира, че всички служители са наясно с рисковете и могат да предприемат подходящи стъпки за защита на цифровите системи и услуги на общинската администрация.

Като цяло, за целите на защитата на шведското електронно правителство, на общинско и централно ниво, държавата е приложила всеобхватен и многопластов подход към киберсигурността, обхващащ различни аспекти

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

на киберзащитата, като управление на риска, мрежова сигурност, кризисна реакция при инциденти, обучение и осведоменост; актуализация на нормативната уредба и регулации.

Високото ниво на технологична напредналост и ресурсна обезпеченост на общинските власти в Швеция, както и на компютърна грамотност на служителите, позволява имплементирането на високи и напредничави технологии за превенция, които в комбинация с високата компетентност в сферата на дигиталните услуги и отговорното поведение на служителите спрямо протоколите за сигурност, показват голяма успеваемост на страната в борбата с основните видове кибератаки срещу публичната администрация. В следствие на това шведските власти отбелязват сравнително малък брой докладвани инциденти, свързани с кражба на пароли за достъп до поверителната информация за гражданите, използващи услугите на електронното правителство.

Белгия

Политиките и мерките на белгийските общински власти в сферата на киберсигурността са в пълна степен синхронизирани с най-добрите практики, залегнали в стратегическата и регулаторна рамка за борба с киберпрестъпленията на ЕС и на останалите държави членки. Подобно на нидерландските си съседи белгийците са водени от разбирането, че никоя индивидуална организация, ИТ експерт или дори цяло правителство не може да се справи само с предизвикателствата пред киберзащитата. Изисква се унифициран, цялостен и синергичен подход, който се базира на инвестиции в образование и квалификация, в иновативност и в публично-частното партньорство.

Един такъв добър пример за смекчаването на щетите и вредите от кибератака в резултат от взаимодействието между публичните организации и частния сектор е мащабната кибератака от май 2022г. Тогава работният процес на над 200 частни и обществени организации като университети, парламентарни, общински и научни институции е засегнат. Официалните източници разкриват, че “Belnet”, базиран в Белгия доставчик на интернет услуги, който се използва широко от обектите на ключовата инфраструктура в страната, е станал обект на “зловреден

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

софтуер" (ransomware). Неизвестни хакери са извършили контролирана атака за отказ на услуга (DDoS), целяща да наруши функционирането на голям набор от електронни услуги чрез претоварване на сървърите с данни.

Наличието на софтуер за ранно идентифициране на зловредно проникване, имплементиран в системата на "Belnet", както и протоколи за кризисна реакция, въведени в частните и публични организации (като университети и общински служби), са довели до почти едновременна и светкавична реакция от всички страни. В резултат на това нападателите не са успели да пробият системите докрай, за да откраднат поверителни данни и пароли. Екипът на "Belnet" е приложил незабавно своите кризисни процедури и се е свързал с Центъра за киберсигурност на Белгия за помощ в овладяването на атаката.

Това е добър пример, показващ как взаимодействието на публичния и частния сектор, координирано от отговорните правителствени органи, и при спазване на единни правила и стандарти за реакция, имплементирани в организационната структура на институциите, са минимализирали въздействието на един много сериозен киберинцидент, потенциално заплашващ кражбата на огромно количество поверителна информация на гражданите.

За да постигне максимална ефективност на мерките за противоборство на киберпрестъпността, националният координиращ орган съблюдава дали унифицираната регулаторна, оперативна и техническа рамка се прилага и спазва повсеместно. Както и горният пример показва, когато това условие е изпълнено, общинската власт, като единица от цялото, може да разчита и да се възползва от експертизата, технологичните достижения, протоколите, реакцията и, ултимативно, защитата от страна на цялата екосистема, заета да подсигурява мрежовата и информационна сигурност на страната. Инвестирането в повишаване квалификацията и осведомеността на служителите за заплахите в кибернетичното пространство и начините да им противодействат са от ключово значение за повишаване цялостната компетенция и способност на администрацията да се пази и да реагира на инциденти. Също толкова ключово е и инвестирането в сътрудничество с ИТ компаниите от частния сектор 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

разработването и имплементирането на продукти и услуги за защита от зловредните дейности в дигиталното пространство.

Белгийските общински власти се придържат към имплементирането на стандартните и задължителни изисквания за сигурност от европейската гледна точка, каквито вече разгледахме и при останалите държави членки. Тези мерки включват използването на защитни стени; системи за откриване и предотвратяване на проникване; методи за криптиране на чувствителни данни и файлове. Освен това общинските власти са имплементирали строг контрол на достъпа до програми, файлове и акаунти, както и система за наблюдение, за да се гарантира, че само упълномощени лица имат достъп до поверителната база данни. Общинските власти разполагат още с планове за реагиране при инциденти и възстановяване след бедствия.

Не винаги е лесно да се оцени ефективността на конкретни взети мерки, тъй като често резултатите от тях са чувствителна информация, която не е публично достъпна, за да не се подпомагат киберпрестъпниците да подобряват своите умения. Освен това, определянето на ефективността на мерките за киберсигурност може да бъде трудна за количествено измерване задача, тъй като зависи от различни фактори. Такива са: естеството и сложността на заплахите; вероятността едно събитие да се е било случило, ако потенциално е било неналично определено защитно средство; както и способността за адаптиране към нови заплахи. Въпреки това, както и горният пример ни показа, Белгия напредва в създаването на ефикасен и координиран метод за противоборство срещу киберзаплахи с обществена значимост, при което си сътрудничат организациите от публичния и частен сектор, под вещата координация на националните органи по киберсигурност.

Полша

Стратегията за киберсигурност на Република Полша за 2019-2024 г., в частта си, засягаща структурите на публичната администрация, е резултат от анализ на настоящи и бъдещи тенденции, предизвикателства и заплахи пред все по-енергичната цифрова трансформация на полската икономика и предоставянето на електронни услуги от общинските власти.

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

Стратегията определя приоритетните области и набелязва мерките, подпомагащи изпълнението на основната цел, която е повишаване на нивото на устойчивост срещу кибернетични заплахи на структурите на публичната власт, както и укрепването на защитата на поверителната информация и база данни. Стратегията залага на публично-частното партньорство и включва всички онези субекти и обекти, които имат достъп до Мрежата и, респективно, са изложени на рисковете и заплахите в киберпространството – ИТ специалисти по сигурността от частния и публичния сектор, потребители и служители. Всички те са опосредствани в изпълнението на задачите от една осъвременена нормативна рамка, ефективни оперативни процеси, както и от модерни информационни технологии.

Приоритетите на полското правителство в областта на информационната сигурност за публичната администрация включват: повишаване на обществената осведоменост относно киберзаплахите; подкрепа на инициативи, насочени към създаване на иновативни решения и инструменти за киберзащита; укрепване на сътрудничеството с частния сектор в разработването на цифрови услуги, използващи нови поколения мобилни мрежи и системи за събиране, анализ и обработка на данни. Ефективността на функционирането на националната система за киберсигурност ще бъде повишена и чрез въвеждане на стандартизация на решенията за сигурност, включително въвеждане на минимални изисквания за сигурност на ИКТ мрежите и системите, оперирани от публичната администрация.

Стратегията също така залага на бюджетни инвестиции в повишаването на човешкия и технологичен капацитет на публичните администрации в борбата с киберпрестъпленията. Структурите на местната власт, изпълняващи обществени задачи, предоставящи обществени услуги и боравещи с поверителна информация на гражданите, са длъжни да включват разходи за киберсигурност в своите финансови планове в съответствие със съответните разпоредби. Детайлният размер и структура на разходите по отделните проекти се определят в процеса на иницииране на конкретни проекти. Оценка на разходите за финансиране по

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

Стратегията за киберсигурност ще се проведе в рамките на Плана за действие.

Източници на финансиране за изпълнение на мерките, заложени в документа, са бюджетите на органите на местната власт, както и средства от националния бюджет и от Европейския съюз.

Планът определя конкретни цели за постигане и разписва мерки за имплементиране от страна на публичната администрация в сферата на киберзащитата.

1. Повишаване нивото на устойчивост на информационните системи на публичната администрация за постигане на достатъчен капацитет за ефективно предотвратяване и реагиране на инциденти. От структурите на местната власт се изисква да следват националните организационни и технически протоколи и стандарти за киберсигурност на: мобилните устройства и приложения; сървърите и мрежите; базата данни; облачните услуги;

2. Повишаване на капацитета в областта на технологиите за киберсигурност. Правителството и местната власт имат за цел да инвестират в инкубирането на промишлени и технологични ресурси за целите на киберсигурността. Това трябва да стане чрез създаване на условия, необходими за развитието на бизнеса, по-специално на МСП и стартиращи фирми, както и институти за научноизследователска и развойна дейност, които се занимават с разработването на нови решения в областта на киберсигурността. Приоритетите включват увеличени възможности в областта на проектирането и производството на софтуер, хардуер и услуги, използвани във всички отрасли на полската индустрия за подобряване на нейната конкурентоспособност. Фокус върху развитието на публично-частното сътрудничество.

3. Изграждане на обществена осведоменост и повишаване степента на компетенции на гражданите и служителите в общинските власти в областта на киберсигурността. Наред с предоставянето на обучение на служителите в публичната администрация с цел по-добро разбиране на заплахите в киберсредата и научаването на способи да им противодействат обучението по киберсигурност трябва да бъде налично възможно най-рано

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 процеса на достъп до цифрови услуги от деца и младежи. По отношение на въпроса за безопасното използване на киберпространството се предполага, че това ще залегне в учебните програми от най-ранна училищна възраст, а учителите ще получат подкрепа при изпълнението на съответната задача, по-специално, чрез актуализиране на своите учебни програми.

Освен това ще се предприемат действия за подпомагане на непрекъснатото професионално развитие на учителите в областта на съвременните технологии и киберсигурността.

Институциите на висшето образование се насърчават да развиват интердисциплинарни специализации, обхващащи управлението на рисковете за информационната сигурност, оценка на защитните механизми на ИКТ системите, защита на личните данни, защита на интелектуалната собственост в Интернет, както и въпроси, свързани с развитието на нови технологии.

Полското правителство е поставило амбициозни задачи и цели пред общинската власт за защита на критичната инфраструктура. В контекста и на днешните събития като военните действия, водещи се на границата на Полша, и активното участие на страната в подпомагането на възпирането на агресията, държавата е изправена пред огромни предизвикателства за киберсигурността си като ежедневни опити за пробиви в системите и кражба на данни. Киберзащитата е възприета на ниво местна власт като кауза с особено голям приоритет заради изключително високата си степен на риск за сигурността.

И все пак, все още е рано, а и трудно да се оцени обективно ефективността на имплементираните мерки, заложени в политиките и стратегията на местните власти за борба с киберпрестъпността. Това е така, защото ефективността на подобни мерки често се определя по това дали евентуална кибератака е щяла да се състои, ако не са били налични определени защитни способи за задържане. Подобни случаи обаче значително по-трудно се докладват, тъй като често протичат без да оставят конкретен маркер в системата за сигурност. Експертите в областта на киберсигурността са категорични, че прилагането на синхронизирани 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

цялостни мерки за превенция на най-често срещаните видове киберинциденти има значително въздействие както количествено, така и качествено върху сигурността на мрежата и информационните системи. Те предпазват от широк набор от киберзаплахи, включително вируси, зловреден софтуер, фишинг атаки и неоторизиран достъп до чувствителни данни.

Румъния

Чувствително нарастналият брой инциденти с киберсигурността на Румъния по време на бурната дигитална трансформация на държавната и общинската администрация, породена от пандемията Covid-19, привлича вниманието на широката общественост към въздействието на кибератаките, които могат да подкопаят и разрушат нормалното функциониране на румънското общество и достъпа до жизненоважни услуги.

Това доведе до необходимостта за актуализация в края на 2021 г. на правната рамка и стратегия за киберсигурност на Румъния. Причините за това са:

1. Непрекъснатата еволюция на кибератаките както от гледна точка на броя, така и от гледна точка на сложността им;

2. Потенциалният регионален или глобален ефект от кибератаките поради взаимосвързаността на услугите;

3. Ускореното развитие на новите технологии (като “интернет на нещата”, изкуствения интелект, машинното обучение, 5G и др.);

4.Откриването на новия европейски промишлен, технологичен и изследователски център за компетентност в областта на киберсигурността в Букурещ, който ще играе важна роля в свързването и координирането на излседователската и развойна дейност в областта на кибернетичните технологии;

В отговор на предизвикателствата, чрез актуализираните си мерки и политики Румъния предвижда да развие и укрепи своите способности за превенция, възпиране и реагиране, както и за устойчивост, включително чрез прилагането на проактивен подход спрямо киберпрестъпността.

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

Стратегията изисква от всички обекти на критичната инфраструктура, сред които е и публичната администрация, да приложат в дейността си конкретни мерки за превенция на заплахите от киберинциденти. Това включва:

1. Сигурни и устойчиви компютърни мрежи и системи. Гарантирането на сигурността и устойчивостта на мрежите и системите е от съществено значение за поддържането на безопасна икономическа и социална среда, особено от гледна точка на защита на дейностите, свързани с електронните услуги и базата данни. Имплементирането на мерките цели да докара мрежовите и информационни системи на общинската власт в съответствие с целите на ревизираната Директива МИС2. Такива мерки са укрепването на механизма за докладване на инциденти, свързани с киберсигурността. Също и създаването на механизми за сертифициране, съответствие и стандартизация в областта на киберсигурността, за по-добро идентифициране на киберрискове и уязвимости на хардуерни и софтуерни продукти;

2. Придържане към консолидираната регулаторна и институционална рамка и активно участие в нейното допълване, подобряване и актуализация. Заложените цели на тази политика изискват да се развият и направят по-ефективни формите на сътрудничество между всички засегнати страна в областта на киберсигурността, като всички участват наравно в изготвянето и укрепването на регулаторната и институционална рамка за киберсигурност.

3. Активно участие в публично-частни партньорства. Целите на тази политика акцентират върху необходимостта от осигуряване на прагматично партньорство между публичните органи и институциите от публичната администрация, частни субекти, академичните среди и научните изследвания и гражданите, за да се създадат синергии и потенциално икономически и социални ползи за цялото общество. Част от мерките предвиждат:

а. Организаирането и провеждането на програми за информиране на обществеността и повишаване нивото на културата на киберсигурност;

б. Разработване на образователни програми в областта на киберзащитата.

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. Провеждане на програми за професионално обучение на лица, които извършват дейности в областта на киберсигурността;

г. Разработване и консолидиране на изследвания в областта на киберсигурността;

д. Провеждане на упражнения с практическа насока и приложимост, в сътрудничество с частната и академичната среда;

Добър практически пример за партньорство между местната власт и академичната среда в целта да се изгради една по-ефективна технологична и оперативна рамка за защита на мрежите и системите е сътрудничеството между общинската власт в университетския град Клуж-Напока и академичните среди.

Започнало като студентски проект в катедрата по компютърни и информационни системи, днес планът и насоките, дело на изследвания на най-добрите и успешни практики от страна на преподаватели и студенти, са приложени като конкретни мерки в политиката на града да защитава по-добре и по-ефективно електронното правителство от заплахи, а също така и поверителните данни за гражданите.

Общинските власти в Клуж-Напока са се фокусирали върху петте най-важни и успешни практики за превенция на основните видове киберзаплахи срещу базата данни и системите на публичната администрация и са ги имплементирали в дейността си:

1. Защитни стени: Защитната стена е система за мрежова сигурност, която наблюдава и контролира входящия и изходящия мрежов трафик въз основа на предварително зададени правила за сигурност. Това е ефикасен механизъм за ограничаване зловредното проникване в системите на общинската власт.

2. Шифроване/криптиране: Шифроването е процес на преобразуване на обикновен текст в нечетлив формат за защита на чувствителни данни или файлове по време на трансфер или съхранение. Препоръчва се всички поверителни информационни потоци на общинската власт да бъдат криптирани и архивирани на допълнителен външен източник.

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

3. Многофакторно удостоверяване и силни пароли: Многофакторното удостоверяване добавя допълнителен слой на сигурност към използването на пароли с голяма степен на сложност, като изисква допълнителна форма на идентификация като например код, изпратен на мобилния телефон или токен устройство.

4. Редовни софтуерни актуализации: Редовните софтуерни актуализации и управление на корекциите са важни за справяне с уязвимостите в защитата на софтуера и операционните системи, които хакерите ежедневно се опитват да пробият и преодолеят.

5. Обучение за информираност относно сигурността: Служителите трябва да бъдат постоянно обучени как да идентифицират и докладват най-актуалните злалахи; как да забелязват и разграничават подозрителната дейност в киберпространството и да следват най-добрите практики за превенция като, например, да не натискат и отварят върху непознати връзки.

Общинските власти в Румъния, като тази в Клуж-Напока, са още един пример за повишаването на степента на осведоменост и осъзнатост за рисковете и заплахите в киберпространството на европейско ниво. Подкрепени и обезпечени от една обновяваща и хармонизираща се регулаторна рамка, в съответствие с европейските директиви и най-добри практики от индустрията, румънските общини напредват в имплементирането на мерки за справяне с комплексния характер на заплахите в кибернетичното пространство. Успешните практики, научени и придобити в резултат от сътрудничеството на местната власт с академичните среди, ИТ индустрията и частния сектор в разработването и въвеждането на нови протоколи, процеси, услуги и продукти в сферата на киберсигурността, водят до положителни резултати, чиято ефективност тепърва ще се анализира и оценя в детайли.

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. Изводи

Глобалната пандемия Covid-19 оказа значително влияние върху увеличаването на киберпрестъпленията и светна като "червена лампа", за уязвимостите на мрежовата и информационна система на публичната администрация. Това е продиктувано от безпрецедентната по своите мащаби и скорост дигитална трансформация на ежедневието, навиците и работния процес на гражданите. В резултат на пандемията много служители започнаха да работят дистанционно, което увеличи използването на слабо защитени домашни мрежи и устройства. Тази промяна в условията на труд улесни киберпрестъпниците да атакуват лица и организации чрез изпитани тактики като фишинг измами, "зловреден софтуер" или социално инженерство. Наяве излязоха проблемите, свързани с недостатъчната ресурсна обезпеченост на общинските власти да поддържат специализиран ИТ персонал и продукти за киберсигурност. В допълнение на това беше отчетена и незадоволителната и неравномерна степен на осведоменост и компетентност на служителите за заплахите в киберпространството.

Макар рисковете за мрежовата и информационна система на електронното правителство от кибератаки да съществуваха и преди пандемията, тя се оказа необходимият лакмус, който да задейства своеобразна революция в осъзнаването и третирането на киберпрестъпността като основна заплаха за националната сигурност на държавите членки в Европейския съюз. Прегледът на законодателството в сферата на киберсигурността ни показа, че всички страни, без изключение, са използвали уроците, научени по време на пандемията, за да актуализират и допълнят своята нормативна уредба в съответствие с новоприетата Директива на Европейския съюз за Мрежова и информационна сигурност, която беше окончателно приета в края на изминалата година.

Значението на МИС2 за повишаването на общото ниво на киберсигурност в ЕС е съществено. Стратегията и разписаните в нея политики и мерки целят да подобрят сигурността и устойчивостта на мрежите, системите и базата данни на публичния и частен сектор от постоянно еволюиращите в своята иновативност и комплексност кибератаки. Директивата, която ще има задължителен характер за страните членки от 2024 година, поставя акцент

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

върху защитата на критичната инфраструкрута и на онези организации и/или индустрии, които осигуряват жизненоважни услуги и продукти за населението. Сред тях се откроява и публичната администрация в контекста на електронните услуги, които предоставя на гражданите. Директивата се фокусира и върху международното сътрудничество в споделянето на опит и информация за противодействие на зловредната дейност в кибернетичното пространство; върху партньорството между държавите членки в изготвянето на холистичен и хармонизиран оперативен и технически инструментариум за противоборство на пробивите в мрежите и базата данни.

От съществена важност е, че държавите членки в ЕС са узрели в разбирането, че киберсигурността има транснационално въздействие и, респективно, трябва да бъде третирана със същия подход. Киберзаплахите не зачитат националните граници и могат да произхождат от всяка точка на света, което затруднява ефективната защита на отделните държави срещу тях. Единствено ако работят заедно, правителствата, частният сектор и гражданите могат да координират успешно усилията за реагиране и да разработват международни споразумения, стандарти и продукти за подобряване на общото ниво на киберсигурност на Общността.

Като се вземе предвид горната теза, е положително да заключим, на база изследването на десет европейски държави за успешните практики, приложени в областта на киберсигурността на публичната администрация, че политиките им се припокриват напълно. Това се оказва и предизвикателство за българската общинска администрация, която трябва да отговори на очакванията и на гражданите, и на европейските си партньори, като имплементира политики и мерки, които да поставят местната ни власт в съответствие с най-добрите стандарти и практики за киберсигурност на Общността.

Експертите в сферата на киберзащитата се обединяват около максимата, че въпросът не е дали мрежите и системите на общинската власт ще станат обект на кибератака, а кога ще се случи това и колко силно ще бъде въздействието. Затова акцентирахме в този доклад върху разглеждането на добрите практики, приложени в публичната администрация на 10 от държавите членки на Общността. Макар да съществуват множество

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

технически и оперативни мерки, които местната власт да предприеме за защита на своята поверителна информация и системи, на база на изследването можем да посочим следните политики, имплементирани в публичната администрация на европейските държави, които се открояват като своеобразен "стандарт". Важно е също така да се отбележи, че нито една от долупосочените мерки не може да защити напълно организацията от кибератаки. Необходимо е да се приложи комбинация от политики за създаване на стабилна екосистема по сигурността. Като също така е важно тези мерки да бъдат преглеждани и актуализирани периодично, за да се гарантира, че са "в крак с времето", както на нормативно, така и на технологично и оперативно ниво.

1/ Силни пароли и многофакторно удостоверяване (MFA): Силната парола е онази, която е свързана с по-голяма степен на сложност, необходима за разбиването ѝ. Включва комбинация от главни и малки букви, цифри и специални знаци. Използването на уникална и силна парола за всеки акаунт може да помогне за защита срещу киберпрестъпления, при които хакерите използват автоматизирани инструменти, за да се опитат да отгатнат или разбият ключовете за достъп. Многофакторната идентификация (MFA) е допълнителен слой на сигурност, който изисква потребителят да предостави две форми на идентификация, преди да получи достъп до акаунт или система. Това може да включва нещо, което потребителят знае, като тайна парола или нещо, което потребителят има, като телефон или токен за сигурност, на който бива изпратен код;

2/ Защитни стени: Защитната стена може да се използва за контролиране и наблюдение на входящия и изходящия мрежов трафик и за блокиране на неоторизиран достъп. Те действат като бариера между компютъра или мрежата и интернет. Могат да бъдат конфигурирани да блокират или разрешават преминаването на определени типове трафик въз основа на правила, зададени от администратора. Това им позволява да блокират злонамерен трафик като опити за хакване, зловреден софтуер и фишинг, като същевременно позволяват преминаването на легитимен трафик;

3/ Системи за откриване и предотвратяване на проникване (IDPS): Представляват технически мерки за сигурност, които са предназначени да откриват и предотвратяват неоторизиран достъп до мрежа или система.

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

IDPS могат да бъдат разделени на две основни категории: системи за откриване на проникване и системи за предотвратяване на проникване. Системите за откриване на проникване са проектирани да идентифицират и предупреждават за потенциални пробиви в сигурността или аномалии в мрежовия трафик, но не предприемат никакви действия за блокирането им. Докато системите за предотвратяване на проникване имат също и способността да предприемат действия за предотвратяване на проникване, като блокиране на злонамерен трафик, "карантиниране" на засегнатите системи или изключване на мрежовата връзка;

4/ Криптиране: Това е метод за защитена комуникация, който използва математически алгоритми за кодиране на данни, файлове, съобщения, така че да могат да бъдат прочетени само от някой с правилния "ключ" за декриптиране. Подобна стъпка затруднява достъпа на неоторизирани потребители до поверителна информация като номера на кредитни карти, идентификационни данни за вход и друга лична информация.

5/ Сегментиране на мрежата: Помага за защита срещу киберпрестъпления, като разделя мрежата на по-малки, изолирани сегменти или „зони за сигурност". Това затруднява хакерите да се "движат" свободно из мрежата, за да получат достъп до чувствителни данни или файлове. Това може допълнително да ограничи потенциалните щети, които нападателят може да причини, ако успее да пробие сегмент от мрежата;

6/ Архивиране на поверителната информация и файлове: Предоставя начин за възстановяване на данни и файлове в случай на успешна атака или кражба. Това може да включва както резервни копия, които се съхраняват извън сайта или в "облака", така и "офлайн" архиви, които се съхраняват на преносим носител;

7/ Информираност и обучение на служителите: 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. Това може да включва предоставяне на обучение по теми като най-добри практики за сигурност, фишинг измами и тактики за социално инженерство. Освен това предоставянето на редовни обучения за текущите

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 актуални заплахи може да спомогне служителите да бъдат бдителни и наясно с най-новите рискове. 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;

8/ Кризисен план за действие при инцидент: Наличието на такъв протокол и план за реагиране може да бъде от изключителна полза за минимизиране въздействието на киберпрестъпления, чрез предоставяне на структуриран и организиран подход за откриване, категоризиране, реагиране, докладване и възстановяване след инциденти със сигурността. Наличието на такъв кризисен план може да помогне за минимизиране на въздействието на даден инцидент чрез предоставяне на ясни насоки за това как да се реагира на различни видове кибератаки, кои са отговорните лица за докладване и действие, какви са сроковете за реакция и т.н.;

9/ Публично-частно партньорство: Както вече разгледахме по-назад в доклада, киберсигурността не е по силите на нито една организация, компания или дори цяло правителство да се справи самостоятелно. Сътрудничеството между публичната администрация, ИТ сектора, гражданското общество, правителството и координиращите органи, както на национално, така и на международно ниво, е ключово. Това се изисква за нуждите от хармонизиране на нормативната база и стандартите за сигурност, а също и за разработването и внедряването на нови услуги и продукти, които ефективно да обезпечават защитата на мрежовата и информационна система в неравната “гонитба” с постоянно еволюиращите техники и методи на хакерите. Сътрудничеството също така е ключово и в областта на обучението и повишаване на компетентностите на служители

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 потребители за това как да се предпазват по-ефективно от рисковете и заплахите в киберпространството;

Анализът на имплементираните мерки в сферата на киберсигурността на публичната администрация показва следното. От една страна, още е твърде рано да се направи категоричен извод за ефективността им, тъй като мнозинството мерки са били имплементирани или относително скоро, или предстои да бъдат имплементирани. Това се налага в съответствие с новоприетата Директива на ЕС МИС2, която добавя публичната администрация към списъка с организациите от критичната инфраструктура, за които ще се отнасят новите, ултимативни и по-строги разпоредби за сигурност на мрежовите и информационни системи. Това изисква и актуализиция на националните законодателства, което, както научихме по-назад в доклада, вече се случва.

От друга страна, оценката на ефективността е не винаги лесна за количествено и качествено измерване. Това е така, защото ефективността на подобни мерки често се определя по това дали евентуална кибератака е щяла да се състои, ако хипотетично не са били налични определени защитни способи за задържане. Подобни случаи обаче значително по-трудно и рядко се докладват, тъй като често протичат без да оставят конкретен маркер в системата за сигурност. Важно е да се спомене също, че голям брой отблъснати кибератаки не се съобщават публично, както от съображения за сигурност на чувствителната информация, която е била атакувана, така и за да не се помага на киберпрестъпниците чрез публичното разкриване на способи и техники за превенция.

Експертите в областта на киберсигурността обаче са категорични, че прилагането на синхронизиран и цялостен набор от технически и оперативни мерки за превенция на най-често срещаните видове киберинциденти има значително положително въздействие, както количествено, така и качествено, върху намаляването на киберинцидентите с последствия и върху подобряване сигурността на мрежовите и информационни системи. Няма методи, които да предотвратяват напълно кибератаките. Но горепосочените мерки са доказани, успешни политики и биха били силен коз в ръцете 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

общинските власти, за да сведат негативното въздействие от потенциални кибератаки до минимум.

Мерките, разписани в този доклад, са определени от експертите в сферата на киберсигурността, както и от отговорните национални и европейски органи, за стандарт в предпазването на публичната администрация и електронното правителство от широк набор от киберзаплахи като, например, вируси, зловреден софтуер, фишинг атаки, социален инженеринг и неоторизиран достъп до чувствителни данни. Важно е обаче 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 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.

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

Използвани източници:

Доклади:

1. “Доклад за напредъка по изпълнение на Актуализираната стратегия за развитие на електронното управление в Република България 2019 - 2025 г. и на мерките от пътната карта за нейното изпълнение”

2. “eGovernment Benchmark 2022”. Author: Capgemini, Sogeti, IDC and Politecnico di Milano for the European Commission Directorate General for Communications Networks, Content and Technology, July 2022

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

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

5. “15 Cybersecurity Best Practices to Prevent Cyber Attacks”. Author: EKRAN, 2022

6. “Nineteen National Cyber Security Strategies. International Journal of Critical Infrastructure Protection”. Author: Eric Luiijf, January 2013

7. “Information security management in German local government”. Authors: Frank Moses, Kurt Sandkuhl, Thomas Kemmerich, 2022

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

9. “OBLIGATIONS ET RESPONSABILITÉS DES COLLECTIVITÉS LOCALES EN MATIÈRE DE CYBERSÉCURITÉ”. Author: Cybermalveillance.gouv.fr, 2022

10. “Local authorities facing cybersecurity issues: What levers for action?” Author: Digital Society Lab France, 2022

11. “Trillion protects Spanish Public Administration against threat of credentials misuse”, Report by Crossword Cybersecurity, 2022

12. “Cybersecurity as a Public Task in Administration”. Author: Katarzyna Chałubińska–Jentkiewicz, October 2021

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

13. “Cybersecurity and Cyberwar”. Author: Peter W. Singer and Allan Friedman, 2014

14. “Cybersecurity Policy Development and Capacity Building – Increasing regional cooperation in the Western Balkans “, Author: Drazen Maravic, 2020

Уебсайтове и линкове:

https://www.enisa.europa.eu

https://academic.oup.com/cybersecurity

https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf

https://www.crosswordcybersecurity.com

https://labo.societenumerique.gouv.fr/en/

https://www.cybermalveillance.gouv.fr

https://www.cnil.fr

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

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

https://postvai.com/cyber/informacionna-sigurnost-estonia.html

https://www.nis-2-directive.com

https://cybersecuritycloud.telefonicatech.com/en/industries/public-admin

https://www.bsi.bund.de/EN/Home/home_node.html

https://www.incibe.es/en/what-is-incibe

https://www.acn.gov.it/en

https://www.mimecast.com/blog/dutch-forge-a-new-cybersecurity-strategy-amid-attacks/

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

https://www.cyberwiser.eu/sweden-se

https://ccb.belgium.be/en/news/cyber-strategy-20-make-belgium-one-least-vulnerable-countries-europe

https://www.law.kuleuven.be/citip/blog/belgium-reboots-cyber-strategy/

https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf

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

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

https://www.verizon.com/business/en-nl/resources/reports/dbir/

https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/netherlands

https://tedangevaare.nl/nl/

https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/digital-public-administration-factsheets

https://www.weforum.org/agenda/2022/12/cybersecurity-european-union-nis/

https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

https://privacyoutloud.ro/articles/romanias-cybersecurity-strategy-a-short-introduction/

https://www.consilium.europa.eu/media/46697/spanish-proposal-to-host-the-european-cybersecurity-industrial-technology-and-research-competence-centre.pdf

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

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