Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

Пътна карта

към

Актуализирана
Национална стратегия за киберсигурност
„КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2023 ”

София, 2021

Съдържание

NB: Всички финансови ресурси са описани без ДДС

Проектна фаза 1: Изграждане на Национална Система за киберсигурност в Република България

Общ необходим финансов ресурс за фазата: 246 020 000 лв.

Проект 1.1. Платформа за интегриране на националните ресурси за киберсигурност на Р. България

Кратко описание:

Проектът ще анализира настоящата ситуация и надгражда съществуващият капацитет на НЦРКИ, като в рамките на проекта ще се изгради чрез надграждане на съществуващи и планирани елементи в интегриран център за оперативно наблюдение на събития свързани с информационна сигурност в държавната администрация в режим 24/7. Този център ще може както да наблюдава събитията в отделни институции, така и да събира, корелира и анализира данни и събития от системи от различни институции. В рамките на проекта ще се изгради и решение на няколко нива, което ще извършва:

- Събиране, съхраняване, корелация и анализ на журнални и мета-данни от активите на конституентите с цел генериране на нотификации за възможни инциденти с киберсигурността
- Събране и анализ на вече генерирани нотификации
- Автоматизиране и управляване на процеса по обработката на сигналите с цел намаляване на необходимият брой служители и времето за реакция и ще позволи интегрирането на конституенти с различен матуритет и технологично ниво на наблюдение.

В рамките на проекта ще бъде и въведено технологична платформа, което сканира и разпознава зловреден код, навлизащ по всички комуникационните канали в инфраструктурата на конституентите. Тази платформа и лаборатория ще разпознава не само вече идентифициран зловреден код, но ще има и възможност за поведенчески анализ в контролирана среда (sandbox), който да идентифицира и непознат до момента malware. Тази среда ще бъде интегрирана в комуникационните платформи и от анализ на потенциален зловреден код при нужда могат да се възползват и други участващи в мрежата конституенти.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена система, която обхваща минимум 3000 актива, 10 000 работни станции с възможност за съхранение на данните 1 година

Източник на финансиране: План за възстановяване и развитие

Проект 1.2. Надграждане на системата за мониторинг на националното киберпространство

Кратко описание:

Проектът включва изграждане на капацитет и компетентност за проактивно наблюдение на националното киберпространство с цел:
- идентифициране на публично достъпни уязвимости
- идентифициране на заплахи, включително и в т.нар. тъмно интернет пространство (dark web)
- идентифициране на слабости в киберсигурността на организациите чрез провеждане на одити и симулации на опити за проникване

В рамките на проекта ще се изгради система от активни интелигентни сензори, които могат да анализират и наблюдават мрежовите потоци от данни, като идентифицират зловреден код, атаки и течове на данни чрез поведенчески анализ с използването на съвременни технологии за машинно обучение. Тези сензори ще бъдат в различни регионални мрежови точки в държавната администрация, и включително ще имат възможност да симулират реални електронни услуги и активи на администрацията с цел идентифициране и анализиране на атаки срещу тях. Събраната информация ще бъде основата за изграждане на цялостна киберкартина, както и генериране на информационен поток с информация за атаките (treatfeed) който ще бъде предоставен на конституентите. Чрез този машинно четим поток администрациите ще могат автоматично проактивно да блокират атаки, които все още не са адресирали тях. Данните, събрани от сензорите ще бъдат съхранявани и в централизирано хранилище за мета-информация. Това хранилище използва технологии за обработка на големи обеми от данни (big data)и съхранява мета-информация, събрана в рамките на работата на националните центрове за наблюдение, от активната сензорна мрежа, както и другите системи и проекти, създаващи информационен поток, описващ събитията в националното кибер-пространство. Натрупаните данни ще бъдат анализирани, за да бъдат идентифицирани макро-тенденции и процеси, както и да бъдат разпознавани софистицирани кибер-заплахи. Тези анализи ще бъдат автоматизирани и ускорени чрез използването на системи с изкуствен интелект. Достъп до хранилището ще бъде предоставен на заинтересуваните институции за научни, R&D и цели на националната сигурност и противодействие на престъпността. Хранилището служи и за основа на изграждането на ISAC (Information Sharing and Analytics Center) съгласно напътствията на ENISA.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: План за възстановяване и развитие
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено наблюдение за минимум 50 организации в различни сектори и региони

Проект 1.3. Обучение и трансфер на знания и способности за поддръжка, администриране и опериране на отделните елементи на платформата и самата платформа като интегрирана среда за киберсигурност

Кратко описание:

В рамките на проекта ще се изгради устойчиво трансфер на знания и изграждане на компетента структура от служители, способни да използват възможностите на системата и да защитават киберпространството на Р. България. Освен обучението под формата на курсове и практически занятия, ще бъдат разработени и онлайн обучителни материали, както и системата от вътрешни правила и процедури описващи процесите според които НЦРКИ ще осъществява реакция на кибер атаки и инциденти.
Ще бъде изградена и симулационна платформа, която позволява симулация в специално отделено виртуализирано пространство на комплексни системи, в което се провеждат комплексни дейности по кибератака и защита (Cyber Range). Такава платформа за симулации ще бъде използвана по множество различни начини:
- за обучение на служители, работещи в областта на кибер-сигурността чрез ситуации, максимално близни до реалността.
- провеждане на мащабни кибер-учения, в които вземат участие представители на множество организации с цел трениране на интер-организационната кооперация.
- провеждане на тествове на системи, оборудване и планове за действие, имащи отношение към националната киберсигурност в напълно контролирана среда
- разработване на системи и планове за действие, имащи отношение към националната киберсигурност

Ще бъдат предприети стъпки за интегрирането на платформата към съществуващи мрежи от такива платформи, което ще улесни участието на национални екипи в международни учения

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: План за възстановяване и развитие
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Обучени минимум 20 служителя за различните роли в НЦРКИ. Проведено минимум едно учение, симулиращо кибер-криза с национален обхват.

Проект 1.4. Кибер защита на Министерство на отбраната

Кратко описание:
Проектът включва изграждане и развитие на капацитет и способности на Центърът по киберотбрана на въоръжените сили на Р България, с цел:

- извършване на проактивно наблюдение на КИС на въоръжените сили, своевременен анализ и оценка на уязвимостите и заплахите в киберпространството.
- осигуряване на оперативна кибер картина и ситуационна осведоменост при изпълнение на мисиите на въоръжените сили;
- намаляване на времето за откриване на киберинциденти и възстановяване на нормалната дейност на КИС на Министерството на отбраната и Българската армия;
- изграждане и развитие на експертен капацитет в областта на киберотбраната, чрез обучение и подготовка, изучаване и въвеждане на добрите практики и оперативни процедури.

Отговорна институция за изпълнението на проекта: Министерство на отбраната

Източник на финансиране: национално и външно финансиране

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изграждане на Център за киберотбрана в МО с пълни оперативни способности.

Проект 1.5. Изграждане на капацитет за изследване и контрол на криптографската и информационната защита на информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност

Кратко описание:
Проектът включва изграждане и развитие на способности на ДАНС в областта на контрола на криптографската и информационната защита с цел:

• извършване на проактивно наблюдение и анализ на механизмите за криптографска и информационна защита на стратегическите обекти и обекти от значение за националната сигурност;

• осигуряване на обективна киберкартина на прилаганите инструменти и механизми за информационна защита в контекста на криптографската сигурност;

• разширяване на съществуващия капацитет на ДАНС по отношение на моделиране, симулиране и проактивно програмиране на мерките за криптографска сигурност и информационна защита;

• осигуряване на необходимата среда (софтуерно и хардуерно осигуряване) за реализиране в максимална пълнота на заложените цели и изследваните модели;

• провеждане на специализирани обучения на служители на ДАНС и служители на стратегически обекти, ангажирани с процеса на създаване, имплементиране, прилагане и контрол на мерки за криптографска сигурност и информационна защита.

Отговорна институция: ДАНС
Източник на финансиране: национално и външно финансиране Индикатори за изпълнение:
Изградени способности на ДАНС за осигуряване на криптографска сигурност и информационна защита на стратегическите обекти и обекти от значение за националната сигурност.
Споделени добри практики и надграждане на съществуващата експертиза на лица ангажирани с процеса на създаване, имплементиране, прилагане и контрол на мерки за криптографска защита в стратегическите обекти и обекти от значение за националната сигурност.
Създадена среда за симулиране на сценарии за въздействие върху информационната сигурност на стратегическите обекти и обекти от значение за националната сигурност.

Отговорна институция за изпълнението на проекта: Държавна Агенция Национална Сигурност

Източник на финансиране:
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ:

Проект 1.6. Повишаване на капацитета за изследване на електромагнитни излъчвания на средства за защита на комуникационни канали и оборудвания в диапазона 100 Hz–18 GHz.

Кратко описание:
Проекта включва повишаване капацитета на ДАНС за изследване на електромагнитни излъчвания на средства за защита на комуникационни канали и оборудвания в диапазона 100 Hz–18 GHz с цел:

• изследване и анализ на механизмите за електромагнитна защита на стратегическите обекти и обекти от значение за националната сигурност;

• осигуряване на обективна киберкартина на прилаганите инструменти и механизми за електромагнитна защита в контекста на електромагнитната сигурност;

• разширяване на съществуващия капацитет на ДАНС по отношение на моделиране, симулиране и имплементиране на мерките за електромагнитна защита на информацията;

• осигуряване на необходимата среда (софтуерно и хардуерно осигуряване) за реализиране в максимална пълнота на заложените цели и изследваните модели;

• провеждане на специализирани обучения на служители на ДАНС в процеса на създаване, имплементиране, прилагане и контрол на мерки за електромагнитна защита на информацията.

Отговорна институция: ДАНС
Източник на финансиране: национално и външно финансиране Индикатори за изпълнение:
Изграждане на способности на ДАНС за осигуряването на електромагнитна защита в диапазона 100 Hz – 18 GHz на комуникационни канали и оборудвания на стратегически обекти и обекти от значение за националната сигурност.
Споделени добри практики и надграждане на съществуващата експертиза на лица ангажирани с процеса на създаване, имплементиране, прилагане и контрол на мерки за електромагнитна и информационна защита в стратегическите обекти и обекти от значение за националната сигурност.
Създадена среда за симулиране на различни сценарии за въздействие на електромагнитните излъчвания на комуникационните устройства на стратегическите обекти от значение за националната сигурност.

Отговорна институция за изпълнението на проекта: Държавна Агенция Национална Сигурност

Източник на финансиране:
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ:

Проект 1.7. Център за научни изследвания, обучения и тренировки в областта на киберсигурността

Кратко описание
Проектът е предназначен за изграждане и развитие на Център за научни изследвания, обучения и тренировки в областта на киберсигурността. Целта е да развиване на капацитет и способности за:
- Подобряване на научните постижения и капацитета за иновации в областта на киберсигурността;
- Регулярно наблюдение, анализ и оценка на критични елементи от националната инфраструктура, имаща отношение към киберсигурността и отбраната.
- Организиране и провеждане на учения в областта на киберсигурността и кибер отбраната на ведомствено и национално ниво с участие на всички заинтересовани структури и организации, имащи отношение към проблематиката;
- Участие и домакинстване, чрез прилежаща инфраструктура, обучени екипи и др., в учения на ЕС и НАТО;
- Провеждане на специализирано обучение в областта на киберсигурността на заинтересовани структури и организации;
- Взаимодействие с ENISA, EDA, NATO и др. организации в областта на научните изследвания, свързани с киберсигурността и отбраната;
- Участие в национални и международни научно-изследователски инициативи и проекти за киберсигурност;
- Функционално тестване на продукти, системи и процеси за киберсигурност;
- Създаване на прототипи за наблюдение, анализ и оценка на кибер обстановката за сигурността и отбраната;
- Осигуряване на научно-изследователска и лабораторна база за анализ, изследване, обучение и прилагане на възможностите за киберзащита и повишаване на сигурността на комуникационно-информационните мрежи и системи;
- Провеждане на тестове, анализи и изследвания на технологии, практики и възможности за провеждане на кибератаки;
- Провеждане на тестове, анализи и изследвания за оценка степента на защитеност на системите и мрежите на МО, БА и на други структури и организации, по отношение на кибератаки и нарушения на сигурността им;
- Осигуряване на възможност за провеждане на научни анализи, изследвания, тестове и измервания на комуникационно-информационно оборудване, разработване на софтуерни приложения и изследване на съвременни технологии и системи за защита на информацията, подходящи за внедряване в изграждани комуникационно-информационни системи на МО, БА и други структури и организации;
- Изследване на способностите на мрежите за противодействие на кибератаки;
- Развитие на способностите за симулиране на кибератаки по мрежите;
- Изграждане на способности за обработка на събития и анализ на рисковете чрез прилагане на системи с изкуствен интелект;

- Изграждане и развитие на научно-изследователски и експертен капацитет на звена от МО, БА и други структури и организации в областта на киберсигурността и киберотбраната.

Отговорна институция за изпълнението на проекта: Институт по отбрана „Професор Цветан Лазаров“, Държавна Агенция „Електронно управление“, Министерство на отбраната.

Индикатори за изпълнение: Изграждане на Център с прилежащи лаборатории за сертифициране на продукти и услуги за киберсигурност с пълни оперативни способности. Акредитиране на центъра от национални акредитационни органи и на ниво ЕС.

Източник на финансиране: национално и външно финансиране

Проект 1.8. Център с прилежащи лаборатории за сертифициране и проверка на съответствието на продукти и услуги за киберсигурност

Кратко описание:
Проектът включва изграждане и развитие на капацитет и способности на Център с прилежащи лаборатории за сертифициране на продукти и услуги за киберсигурност, с цел:

- Оценяване на изпълнението на специфицираните изисквания, свързани с ИКТ продукт, ИКТ услуга или ИКТ процес.
- Оценяване на съответствието съгласно действащите европейски и/или национални схеми за сертифициране на киберсигурността на софтуерно базирани продукти, услуги и процеси.
- Оценяване на съответствието съгласно действащите европейски и/или национални схеми за сертифициране на киберсигурността на хардуерно базирани продукти, услуги и процеси.
- Оценка на електромагнитните излъчвания на ИКТ продукти, ИКТ услуги и ИКТ процеси
- Оценка на електромагнитната съвместимост на ИКТ продукти, ИКТ услуги и ИКТ процеси
- Изграждане и развитие на експертен капацитет в областта на киберотбраната, чрез обучение и подготовка, изучаване и въвеждане на добрите практики и процедури за сертификация.

Отговорна институция за изпълнението на проекта: Институт по отбрана „Професор Цветан Лазаров“, Държавна Агенция „Електронно управление“, Министерство на отбраната

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изграждане на Център с прилежащи лаборатории за сертифициране на продукти и услуги за киберсигурност с пълни оперативни способности. Акредитиране на центъра от национални акредитационни органи и на ниво ЕС

Източник на финансиране: национално и външно финансиране

Проектна фаза 2: Изграждане на система за киберзащита на споделените информационни ресурси

Общ необходим финансов ресурс за фазата: 178 537 000 лв.

Проект 2.1. Защитено споделено информационно пространство на електронното управление (ЗСИПЕУ)

Кратко описание:

Проекта ще изгради Защитено споделено информационно пространство на електронното управление (ЗСИПЕУ), което да позволи централизирано интелигентно управление на информационните ресурси на електронното управление

Основни дейности по проекта включват:

1: Създаване на защитено споделено информационно пространство за е-управление.

1.1. Проектиране на архитектурата на ЗСИПЕУ, основана на анализ на добри практики, приложими на национално ниво, както и на наличните вече технологични компоненти в ДХЧО и ЕЕСМДАНС, чрез които се гарантира изпълнението на заложените в проекта цели.

1.2. Придобиване на необходимото оборудване за обезпечаване на комуникационна свързаност и защита (вкл. при необходимост алтернативна свързаност до центровете за данни).

1.3. Осигуряване на необходимите допълнителни технически средства за централизирано управление на СИР в администрациите, които се присъединяват.

1.4. Изграждане на елементите от централния компонент в центровете за данни, необходими за реализиране на целите на проекта (вкл. проектиране, доставка, конфигуриране).

1.5. изграждане и конфигуриране на ЗСИПЕУ, включително конфигуриране на централния компонент и оборудването в администрациите чрез внедряване на системи за сигурност и електронна идентификация и оторизация, управление на информация и събития за сигурност и пр.

Дейност 2: Присъединяване и интегриране на публични структури и техни ресурси към ЗСИПЕУ:

2.1. Присъединяване на администрацията към ЗСИПЕУ, в това число към системата за централизирано управление на идентичности и оторизация и системите за мониторинг.

2.2. Интегриране на инфраструктура и информационни ресурси на администрацията към защитеното споделено пространство.

2.3. Осигуряване на отдалечен достъп на определени служители от администрацията до ресурси в ЗСИПЕУ.

2.4. Осигуряване на система за сигурност на крайните устройства на публичните структури (EDR) и осигуряване на разширено URL филтриране независимо от локацията за предварително дефиниран брой държавни служители.

В рамките на проекта ще се извърши и специализирани обучения на администратори.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено ЗСИПЕУ в 1200 административни сгради, в които е изградена локална инфраструктура на пространството, управлявана от централна компонента за администриране на мрежовите сегменти, осигурена възможност за работа с отдалечен достъп чрез ЗСИПЕУ на 30% служителите в държавната администрация.

Проект 2.2. Въвеждане на системи за сканиране за уязвимости и пропуски в киберсигурността

Кратко описание:

Ще бъде разработена система за сканиране за уязвимости на системите и приложенията, работещи в рамките на споделените ресурси и система и процес за тяхното управление. Установените уязвимости ще бъдат елиминирани, чрез промени в системите, а при невъзможност уязвимите системи ще бъдат защитени чрез конфигуриране на защитите на мрежово и приложно ниво, включително филтриране на web трафик

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена система и сканирани минимум 25 приложения и системи

Проект 2.3. Въвеждане на решения за поддържане на резервни копия на системни компоненти на системата, с цел бързо възстановяване при отпадания в резултат на киберинциденти

Кратко описание:

Платформата ще създава автоматично архивни и резервни копия на системните компоненти, като ще позволява гъвкавост на настройките, както и автоматизирано възстановяване на един или множество компоненти.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена система и обхванати минимум 30 компонента

Проект 2.4. Изграждане на автоматизирана киберзащита на уеб-базирани приложения чрез специализирани защитни стени

Кратко описание:

Изграждане на плаформа, която да защитава уеб-базираните приложения от атаки на приложно ниво. С цел ускоряване на въвеждането на защитата, в комплексната среда на множество приложение, платформата ще има възможност за автоматично самообучение, анализ на поведението и разпознаване на аномално поведение и атаки след преминаване в режим "Защита".

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена система и обхванати минимум 15 уеб базирани приложения

Проект 2.5. Управление на привилегирован достъп до системите и сървърите, чрез защита на акаунтите с администраторски достъп

Кратко описание:

Платформа, която позволява управлението на привилигирования достъп до сървърни, комуникационни и системните компоненти, намиращи се в рамките на споделените ресурси. Платформата ще позволява управление на всички привилигировани потребители и пароли, управление на процеса за достъп (заявление, одобрение, запис на действията на потребителя в системата, подмяна на пароли и др.) и ще служи за адресиране на риска от компрометиране ан привилигирован достъп, както и недоброномерен служител с повишени права. Платформата ще пази журнални логове съгласно нормативните изисквания.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена платформа, обхващаша всички сървърни, комуникационни и споделени ресурси

Проект 2.6. Анализ на кода на приложения с цел отстраняване на уязвимости и пропуски в сигурността допуснати приразработване или функционално надграждане

Кратко описание:

Изграждане на капацитет и платформа за анализ на изходният код на системите и приложенията, които се въвеждат в употреба в рамките на споделените ресурси. Развитие на платформата за съхранение на изходен код и реализиране на автоматизирани способности за анализ. Въвеждане и утвърждаване на процеси по управление на промени при системите и приложенията, въведени в експлоатация в рамките на споделените информационни ресурси и осигуряване на спазването на нормативните изисквания.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена платформа и анализирини най-малко 5 системи

Проект 2.7. Повишаване на киберсигурноста на споделените ин формационни ресурси чрез анализ и контрол на DNS заявките от сървърите, на база принадлежност към дадена категория, риск или репутация.

Кратко описание:

Изграждане на платформа, която анализира и филтрира DNS заявките, като се използват комерсиално и некомерсиално достъпни бази данни, информационни потоци и източници, за да се блокира достъпа от и към рискови зони в кибер-пространството. Платформата ще е федерирана, за да може да се осигури устойчивост и производителност в рамките на работата на споделените информационни ресурси.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена и функционираща платформа

Проект 2.8. Изграждане на система за оркестрация и управление на информация и събития за киберсигурност на споделените информационни ресурси

Кратко описание:

В рамките на проекта ще се изгради система, която събира и анализира аларми и нотификации за събития свързани с информационната сигурност в споделените ресурси и оркестрира и автоматизира процесът по техният анализ и обработване. Ще бъдат разработени и въведени стандартни работни процедури.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена система и разработени процедури за работа

Проектна фаза 3: Повишаване капацитета на Националните компетентни органи (НКО) и Секторните екипи за реагиране при инциденти с компютъраната сигурност към тях (СЕРИКС)

Общ необходим финансов ресурс за фазата: 109 000 000 лв.

Проект 3.1. Повишаване капацитета на НКО и СЕРИКС в сектор Енергетика

Кратко описание:

Изграждане на самостоятелни НКО и СЕРИКС в сектор Енергетика, включително обособяване и оборудване на помещение, осигуряване на ИТ инфраструктура (сървъри, софтуер и работни станции). НКО и СЕРИКС трябва да са интегрирани и да работят съвместно и подмогнати от национално ниво, но да имат капацитета да работят самостоятелно. При първоначалното изграждане функционалността ще се поеме от Националния компетентен орган за всички административните органи (ДАЕУ) и Националния екип за реагиране при инциденти с компютърната сигурност, като постепенно ще се прехвърлят към Секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС).

Отговорна институция за изпълнението на проекта: Министерство на Енергетиката
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено НКО и СЕРИКС в сектор Енергетика

Проект 3.2. Повишаване капацитета на НКО и СЕРИКС в сектор Транспорт и доставчици на цифрови услуги

Кратко описание:

Изграждане на самостоятелни НКО и СЕРИКС в сектор Транспорт и доставчици, включително обособяване и оборудване на помещение, осигуряване на ИТ инфраструктура (сървъри, софтуер и работни станции). НКО и СЕРИКС трябва да са интегрирани и да работят съвместно и подмогнати от национално ниво, но да имат капацитета да работят самостоятелно. При първоначалното изграждане функционалността ще се поеме от Националния компетентен орган за всички административните органи (ДАЕУ) и Националния екип за реагиране при инциденти с компютърната сигурност, като постепенно ще се прехвърлят към Секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС).
Отговорна институция за изпълнението на проекта: Министерство на Транспорта, Информационните технологии и Съобщенията
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено НКО и СЕРИКС в сектор Транспорт и доставчици

Проект 3.3. Повишаване капацитета на НКО и СЕРИКС в сектор Доставка и снабдяване с питейна вода

Кратко описание:

Изграждане на самостоятелни НКО и СЕРИКС в сектор Доставка и снабдяване с питейна вода, включително обособяване и оборудване на помещение, осигуряване на ИТ инфраструктура (сървъри, софтуер и работни станции). НКО и СЕРИКС трябва да са интегрирани и да работят съвместно и подмогнати от национално ниво, но да имат капацитета да работят самостоятелно. При първоначалното изграждане функционалността ще се поеме от Националния компетентен орган за всички административните органи (ДАЕУ) и Националния екип за реагиране при инциденти с компютърната сигурност, като постепенно ще се прехвърлят към Секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС).

Отговорна институция за изпълнението на проекта: Министерство на Регионалното Развитие и Благоустройството

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено НКО и СЕРИКС в сектор Доставка и снабдяване с питейна вода

Проект 3.4. Повишаване капацитета на НКО и СЕРИКС в сектор Здравеопазване

Кратко описание:

Изграждане на самостоятелни НКО и СЕРИКС в сектор Здравеопазване, включително обособяване и оборудване на помещение, осигуряване на ИТ инфраструктура (сървъри, софтуер и работни станции). НКО и СЕРИКС трябва да са интегрирани и да работят съвместно и подмогнати от национално ниво, но да имат капацитета да работят самостоятелно. При първоначалното изграждане функционалността ще се поеме от Националния компетентен орган за всички административните органи (ДАЕУ) и Националния екип за реагиране при инциденти с компютърната сигурност, като постепенно ще се прехвърлят към Секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС).

Отговорна институция за изпълнението на проекта: Министерство на Здравеопазването

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено НКО и СЕРИКС в сектор Здравеопазване

Проект 3.5. Повишаване капацитета на НКО и СЕРИКС в сектор Банково дело

Кратко описание:

Изграждане на самостоятелни НКО и СЕРИКС в сектор Банково дело, включително обособяване и оборудване на помещение, осигуряване на ИТ инфраструктура (сървъри, софтуер и работни станции). НКО и СЕРИКС трябва да са интегрирани и да работят съвместно и подмогнати от национално ниво, но да имат капацитета да работят самостоятелно. При първоначалното изграждане функционалността ще се поеме от Националния компетентен орган за всички административните органи (ДАЕУ) и Националния екип за реагиране при инциденти с компютърната сигурност, като постепенно ще се прехвърлят към Секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС).

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено НКО и СЕРИКС в сектор Банково дело

Проект 3.6. Укрепване капацитета на НКО и СЕРИКС в сектор Инфраструктури на финансовия пазар

Кратко описание:

Изграждане на самостоятелни НКО и СЕРИКС в сектор Инфраструктури на финансовия пазар, включително обособяване и оборудване на помещение, осигуряване на ИТ инфраструктура (сървъри, софтуер и работни станции). НКО и СЕРИКС трябва да са интегрирани и да работят съвместно и подмогнати от национално ниво, но да имат капацитета да работят самостоятелно. При първоначалното изграждане функционалността ще се поеме от Националния компетентен орган за всички административните органи (ДАЕУ) и Националния екип за реагиране при инциденти с компютърната сигурност, като постепенно ще се прехвърлят към Секторните екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС).

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградено НКО и СЕРИКС в сектор Инфраструктури на финансовия пазар

Проект 3.7. Интегриране на оперативни центрове за киберсигурност на телекоми и оператори на критична инфраструктура с Национален екип за реагиране при инциденти с компютърна сигурност

Кратко описание:

Изграждане на платформа, която да интегрира информационните потоци от центровете за киберсигурност на Телекомуникационни оператори и оператори на критична инфраструктура, включително обмен на аларми за потенциални събития за кибер-инциденти, мета-данни за трафични потоци и информация за ранни предупреждения.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена интеграция и обмен на данни между оперативните центрове на телекомите и операторите и НЕРИКС

Проект 3.8. Повишаване на нивото на мрежовата и информационна сигурност при субектите по чл 4 ал 1 т. 3 и 4 от Закон за Киберсигурност;

Кратко описание:

Разработване на типизирано решение за осигуряване на кибер-сигурността на административните органи и операторите на съществени услуги и доставчиците на цифрови услуги във сектор, подсектор и услуги, посочени в приложения № 1 и 2 на ЗКС, както и лицата, осъществяващи публични функции, които не са определени като оператори на съществени услуги, когато тези лица предоставят административни услуги по електронен път, организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на този закон, когато тези организации предоставят административни услуги по електронен път.. Тези типизирани решения ще бъдат разработени в три "размера" и ще улеснят организациите да развият и бързо да подобрят кибер-устойчеивостта си. Ще бъде направен анализ и типизирано решение ще бъде внедрено в няколко от целевите организации, след което ще бъде предадено на тяхното управление.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Разработени три типизирани цялостни решения, въведени в експлоатация в минимум 5 организации.

Проект 3.9. Провеждане на национални и секторни кибер учения

Кратко описание:

Ще бъде изградена разширена платформа (Cyber Range), която позволява симулация в специално отделено виртуализирано пространство на системи, включително специфични такива, които попадат в обхвата на секторните ЕРИКС и екипи, като например SCADA системи, IoT и д.р. В тази платформа ще се се провеждат симулации на комплексни дейности по кибератака и защита. Такава платформа за симулации ще бъде използвана по множество различни начини:

- чрез разработени сценарии, специфични за участващите сектори - за обучение на служители, работещи в областта на кибер-сигурността чрез ситуации, максимално близни до реалността.
- провеждане на секторни и междусекторни кибер-учения, с цел изграждане на междуорганизационна кооперация
- разработване на системи и планове за действие, имащи специфични за киберсигурността в участващите сектори.

В платформата ще бъдат създадени сценарии, които обхващат симулации, включващи специфични системи, заплахи и събития за секторите, включително и транс-секторни сценарии

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Разработени минимум 3 секторни сценария и проведени минимум 2 обучения

Проект 3.10. Изграждане на Национален компетентен орган/и по киберсигурност

Кратко описание:

Ще се изгради необходиматата инфраструктура, сървърни, комуникационни системи, включително необходимите работни станции и ще се разработят нужните платформи за обслужването на дейността на новосъздадения НКО. Ще се изгради капацитет и процедури за работа.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изграден и работещ НКО по Киберсигурност

Проектна фаза 4: Изграждане на колаборативна среда за повишаване на партньорското доверие и сътрудничество в областта на киберсигурността на национално ниво

Общ необходим финансов ресурс за фазата: 6 000 0000 лв.

Проект 4.1. Създаване на партньорска мрежа за колективна реакция при компютърни атаки срещу българското кибер пространство

Кратко описание:

В рамките на проекта ще се изгради необходимата инфраструктура (системи, платформи и др.) които да позволяват на доброволните участници в партньорската мрежа да обменят информация по сигурен и управляем начин. Платформите и стандартните процедури за работа ще бъдат разработени след проучване на нуждите и желанията на потенциалните участници.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Работеща партньорска мрежа, в която участват минимум 5 организации

Проект 4.2. Изграждане на автоматизирана среда за споделяне на информация за уязвимости с български и международни партньори

Кратко описание:

Ще бъде изградена автоматизирана система, която да позволява ефективното разпространение на информация за уязвимости и информация за ранно предупреждение за кибер инциденти между партньорите, участващи в доброволната мрежа.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Работеща автоматизирана платформа, в която са включени минимум 5 организации

Проект 4.3. Разработване на система за разпространение и промотиране на препоръки за киберзащита и информация в областта на киберсигурността

Кратко описание:

Ще бъде изградена платформа за събиране, разпространенеи и промотиране на препоръки за кибер защита, информация и стандартни процедури в областта на киберсигурността. Разработените препоръки ще са детайлни и ще следват нормативните и регулационни изисквания, така че да предоставят улеснение и да ускоряват постигането на матуритет по отношение на киберсигурността.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Работеща платформа за разпространение на информация

Проект 4.4. Въвеждане и налагане на контрол по Европейския механизъм за прилагане на европейските схеми за сертифициране в областта на киберсигурността съгласно Акт за киберсигурност Регламент (ЕС) 2019/881

Кратко описание:

Изграждане на необходимата функционалност за контрол на сертификационните процеси в областта на киберсигурността в съответствие с Европейския механизъм за контрол. Изграждане на цялостната необходима инфраструктура, включително разработване на нормативните мерки, независими платформи, сървърни системи и работни станции на служители. Синхронизация на дейността и осигуряване на кооперация с Българска служба за акредитация.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изградена функционалност за контрол.

Проект 4.5. Организиране и провеждане на киберучения и специализирани обучения в партньорски мрежи за киберсигурност

Кратко описание:

Ще бъде разработена програма за обучение, базирана на анализ на нуждите и недостига на квалифицирани служители в обхванатите организации. На базата на разработената програма ще се проведат планираните учения и обучения за придобиване и повишаване на уменията, като по този начин ще се адресира недостига на работна ръка в областта.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Обучени минимум 50 човека.

Проект 4.6. Налагане на кодекс и правила за кибер етика като вътрешни правила и етичен кодекс на служителите и гражданите

Кратко описание:

Разработване на кодекс и правила за кибер етика и провеждане на разпространителска и разяснителна кампания, която да промотира приемането на подобни вътре-секторни и вътре-организационни документи.

Отговорна институция за изпълнението на проекта: Министерски Съвет
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Разработени примерни етичен кодекс и правила за кибер етика

Проектна фаза 5: Изграждане на защитена киберсреда среда за уязвими бизнеси и организации

Общ необходим финансов ресурс за фазата: 67 000 000 лв.

Проект 5.1. Внедряване на централизирани системи и решения за наблюдение на крайни станции с възможност за разпознаване на „непознати атаки“ (zero-day), базирани на поведенчески анализ на потребителите и системните процеси

Кратко описание:
В рамките на проекта ще бъдат разработени няколко типови архитектури за защита на малки и средни предприятия, които нямат необходимият капацитет за изграждането на подобни системи. Архитектурите ще бъдат централизирани и ще целят пълно спазване на нормативните и регулационните изисквания, както и ще включват стандартни процедури за работа за улесняване на организацията. Ще бъде проведено проучване и ще бъдат идентифицирани организации на които да бъде предложено да получат система за кибер-защита изградена спрямо типовите архитектури.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Разработени минимум 3 типови архитектури, които да бъдат имплеменирани в най-малко 5 различни организации.

Проект 5.2. Организиране и провеждане на информационни кампании, събития и инициативи, насочени към повишаване на кибер-хигиената в цифровата икономика и цифровото общество.

Кратко описание:

В рамките на проекта ще бъдат разработени няколко информационни кампании, целящи повишаването на осведомеността и киберхигиената, като например:

- кампания, целяща разясняване на основната киберхигиена при работа с основните информационни инструменти на киберпространството
- кампания, целяща разясняване на киберхигиента при обмен на лична и конфиденциална информация, включително с държавната администрация
- кампания целяща осъзнатост по отношение на съвременните киберзаплахи и необходимите мерки на киберхигиена за да се предпазим от тях

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Проведени кампании, които са адресирали минимум 50 000 гражданина

Проект 5.3. Създаване на информационна система за оценка на рисковете в организации и предприемане на мерки за покриването им

Кратко описание:

Ще бъде разработена информационна система, която улеснява анализа и оценката на рисковете по отношение на киберсигурността съгласно нормативните изисквания. Тази система ще бъде интегрирана със съществуващите регистри на информационните активи, както и ще бъде постоянно обновявана по отношение на рисковете в националното киберпространство. По този начин ще може да бъде осъществена бърза и точна оценка на рисковете, което пък от своя страна ще доведе до изграждане на система за адекватна и ефективна киберзащита в организациите.

Отговорна институция за изпълнението на проекта: Държавна Агенция „Електронно управление“

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: разработена информационна система, въведена в употреба

Проектна фаза 6: Повишаване на мрежовата и информационна сигурност във вътрешната и външна инфраструктура на МВР с цел защита на публичните услуги, предоставяне на граждани, административни органи и бизнес организации

Общ необходим финансов ресурс за фазата: 43 650 000 лв.

Проект 6.1. Изграждане на център по киберпрестъпност в ГДБОП-МВР

Кратко описание:
Центъра по киберпрестъпност в ГДБОП-МВР се явява единствената национално компетентна структура в България, която противодейства на киберпрестъпността.
Създаването на Центъра ще позволи адекватно, навременно и качествено разследване и разкриване на компютърни и компютърно-свързани престъпления.
Развиването на компетенции в Центъра ще позволи и надеждна комуникация с международните партньори, ангажирани с противодействието на киберпрестъпността.
Предвижда се изграждането на нов сграден фонд, в който да се помести Центъра, както и снабдяването му с необходимия човешки и технически капацитет.

Отговорна институция за изпълнението на проекта: ГДБОП-МВР

Източник на финансиране: Фонд Вътрешна сигурност

ИНДИКАТОРИ ЗА ИЗПЪЛНЕНИЕ: Изграден център по Киберпрестъпност в ГДБОП-МВР

Проект 6.2. Изграждане на Център за управление на сигурността на информационните и комуникационни системи в МВР (Security Operation Center – SOC и Security Orchestration, Automation and Response - SOAR)

Кратко описание:

Министерството на вътрешните работи (МВР) се явява едно от най-критичните ведомства по отношение информацията и регистрите, които обслужва. Регистрите и информационните системи и услуги, предоставяни от МВР, работят както във вътрешната, така и във външната инфраструктура на МВР. Компрометиране на някой от тях може да доведе до компрометиране на националната сигурност на държавата, както и на данните на голям брой български граждани. Допълнително МВР е структура в държавата, която е отговорна за защитата на населението при бедствия и аварии, в това число и кибератаки срещу българските информационни ресурси. ДКИС към МВР спрямо вменените функционални задължения, осигурява защитата на критичната инфраструктура от национално значими информационни ресурси – база данни и IT услуги, които участват в обменът между държавни институции и административни органи, осъществяващи публични функции.

Отговорна институция за изпълнението на проекта: ДКИС- МВР

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

Индикатори:

- изграден център с възможност за обмен на информация с Националния CERT, както и с центровете за реакция при инциденти, свързани с информационната сигурност;
- гарантирана защита на данните на българските граждани чрез прилагане на средства за защита и проследимост на използването на информацията за тях;
- мониторинг и анализ на мрежовия трафик към информационните активи във вътрешната и външна инфраструктура на МВР, с цел превенция и навременно откриване на потенциално разпространение на зловреден код и атаки към ресурсите, използвани от гражданите, целящи компрометиране на техните данни и отказ на услугите;
- превръщане на МВР в съществен участник в интегрираната национална екосистема за кибер сигурност, в съответствие с Актуализираната стратегия за киберсигурност „Киберустойчива България 2023“.

Проект 6.3. Надграждане на защитни стени, осигуряващи сигурен и защитен достъп до електронни услуги в публичния сегмент на МВР.

Кратко описание:

Предимствата на защитните стени от следващо поколение е използването на задълбочена проверка на пакети за идентифициране и управление на приложения, независимо от IP порта, използван от приложението. Други предимства са ефективно откриване на инциденти, по-малко време за реакция и по-ефективна кибер защита. Deep Packet Inspection (DPI) е основна функция на на защитните стени от следващо поколение стените. Тя изследва съдържанието на входящите и изходящите пакети данни за злонамерен софтуер и други заплахи, преди да ги препрати.

Съвременният интернет все повече използва стандарт за криптиране, наречен TLS 1.3. Защитните стени от следващо поколение напълно дешифрират и инспектират пакети с данни, криптирани с TLS 1.3, давайки по-голям контрол на сигурността и спиране на заплахи тип “нулев ден”.

Отговорна институция за изпълнението на проекта: ДКИС- МВР

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

Индикатори:

- надграждане на защитата на инфраструктурата на МВР, което ще гарантира защитата от кибератаки и заплахи на публичните услуги, и доведе до повишаването на мрежова и информационна в интернет инфраструктурата на МВР;
- криптираният SSL трафик защитава клиентите, интернет и сървърите на приложения от криптиран трафик със злонамерен SSL код, който много устройства за сигурност не откриват.

Проект 6.4. Защита от кибератаки и заплахи на крайни потребители в мрежите на МВР (End Point protection)

Кратко описание:

В ежедневната борба срещу киберпрестъпността се изискват решения, които предоставят пълна видимост на всички крайни точки във външната и вътрешна инфраструктура на МВР. Целта е да се събират ценни данни, за да може да се открие, анализира и реагира адекватно на всякакъв тип атаки. За да се постихне това следва да се подмени базовата анти-вирусна защита и да се изгради под-система за защита на крайно клиентските устройства/потребители от следващо поколение, базирана на изкуствен интелект (AI) и машинно обучение (Machine learning), с които предотвратява, открива и отменя, както всички познати заплахи, така и непознати заплахи (Zero-Day заплахи). Технологията е позната като Advanced Endpoint Protection (AEP). За целта се разчита на изкуствен интелект и автономни решения, които да реагират на заплахите мигновено и се задействат незабавно при откриване на атака. Обединяването на тези функционалности в един агент, разположен на крайното устройство, комбинирайки автоматични защитни мерки, помага на екипите за сигурност при анализа на инциденти и по този начин оптимизира тяхната работа.

Отговорна институция за изпълнението на проекта: ДКИС- МВР
Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)
Индикатори:

- защита на клиентите в инфраструктура МВР от Zero-Day заплахи;
- възможност за откриване на софтуер с уязвимости, който е инсталиран в мрежата на организацията;
- Rollback функционалност за допълнително повишаване нивото на сигурност, което позволява в случай на заразяване с криптиращ вирус (Ransomware), лесно и бързо да възстановите заразената машина до напълно функционираща среда, изчистена от заплахата;
- гъвкаво мащабиране за крайни клиентски устройства и централизиран мениджмънт.

Проект 6.5. Система за управление на уязвимости на информационните и комуникационни системи на МВР

Кратко описание:

Мащабите, честотата и въздействието на инцидентите свързани със сигурността се увеличават и представляват огромна заплаха за функционирането на мрежите и информационните системи във вътрешната и външна инфраструктура на МВР. Министерството на вътрешните работи (МВР) се явява едно от най-критичните ведомства по отношение информацията и регистрите, които обслужва. Компрометиране на някой от тях може да доведе до компрометиране на националната сигурност на държавата, както и на данните на голям брой български граждани. Основна цел на проекта е осигуряването на информационна сигурност на масивите от данни и системи, управлявани от МВР, автоматизиране на процеса за управление на уязвимостите в мрежата и тестване на сигурността на информационни системи чрез единна платформа чрез изграждане на под-система за управление на слабости и/или уязвимостта (технология за Vulnerability management).

Системата за Управление на уязвимости осигурява, проверява и подпомага навременно познание за служителите относно наличие на пропуски в системите или устройствата в мрежата на МВР. Целта е чрез нея да се осигури непрекъснато усъвършенстване на информационните системи и услуги, чрез предоставяне на доклади за последните налични от производители софтуерни ъпдейти и подобрения, ъпгрейди и актуализации за наличните системи в мрежата, навременно отстраняване на пропуски или проблеми за различните по тип устройства в мрежата. Софтуерът за управление на уязвимости ще даде видимост върху всички разработени, интегрирани и използвани в инфраструктурата информационни активи. По този начин ще се постигне непрекъсваемост в работата на информационните системи по в съответствие с ISO 22031, както и защита на информацията в тях, съгласно Европейския регламент за защита на личните данни (GDPR).

Отговорна институция за изпълнението на проекта: ДКИС- МВР

Източник на финансиране: Програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ (ПНИИДИТ)

Индикатори:

- ще се подобри управлението на сигурността на информацията чрез разпределение на отговорностите за извършваните дейности - управление на риска, управление на информационните активи, управление на инцидентите, управление на достъпите (логически) и др.

чрез повишаване на нивото на киберзащита в МВР и ще се повиши и сигурността на комуникационно-информационна среда за безпроблемното и ефективно изпълнение на служебните задължения на служителите в МВР.