ISSN 2738-7089 https://doi.org/10.11610/cybsec09bg

Funded by the European Union

Digital Innovation Hub Trakia

ИИКТ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Информационен бюлетин за киберсигурност

Бюлетин Септември 2023 Номер 9

Цели и обхват

Съдържание:

- Цели и обхват
- Фокус на изданието
- Кибер полигони и симулатори като средства за обучение
- Кибер устойчивост по опита на NCI Academy
- Онлайн платформи за обучение по киберсигурност през 2023
- Cybersecurity for Decision Makers
- Посещение на Министърът на труда и социалната политика в обучителния център на ЕЦИХ „Тракия"
- Европейска организация за киберсигурност (ECSO)
- Връзки към институции и инициативи
- Редакционен съвет

Настоящия брой на информационния бюлетин за киберсигурност е ориентиран към кибер-полигоните и симулаторите като средства за обучение. Тази тематика е във фокуса на провежданите обучения от ЕЦИХ Тракия, в резултат на изградените връзки между местната публична администрация, бизнеса и академичните среди.

Крайна цел при формирането на екосистемата на ЕЦИХ Тракия е изграждане на академия за дигитална (цифрова) трансформация и кибер устойчивост. Това може да се реализира като се обединят всички услуги за кибер-образование, обучение и тестване, предоставяни от ЕЦИХ Тракия. За целта освен провежданите обучения е необходим и кибер-полигон. Кибер-полигонът като симулирана среда играе важна роля за едновременно извършване както обучения за ситуационни операции, така за реализиране на тестове и изследвания с образователна цел. Описани са основните компоненти на кибер полигона като симулатор за обучение и тестване. Представен подходът, използван от академията по кибер сигурност ThinkCyber, при който обучението, упражненията и изпитите са базирани на актуалните кибер заплахи в реалния свят.

В броя е представен опита на NCI Academy (NATO Communications and Information Academy), акредитирана за осигуряване на качество като център за образование и обучение на НАТО. Представен е линк към каталога от услуги/курсове, предлагани за обучение в киберпространството от NCI Academy.

Представени са някои от известните онлайн платформи за обучение по киберсигурност през 2023 г., безплатни и платени в зависимост от курса и други фактори. В броя е представено и първото издание на книгата "Cybersecurity for Decision Makers".

Отразено е посещението на Министърът на труда и социалната политика – д-р Иванка Шалапатова, която посети обучителния център на Европейския цифров иновационен хъб „Тракия" по покана на ръководството на Съюза за стопанска инициатива (координатор на проекта по програма Цифрова Европа за европейски цифрови иновационни хъбове).

В настоящия брой е представена Европейската организация за киберсигурност (ECSO), която допринася за развитието на общности за киберсигурност и изграждането на европейската екосистема за киберсигурност.

Редактор на броя: **проф. д.н. Даниела Борисова**

Фокус на изданието:
Кибер полигони и симулатори като средства за обучение

Гл. ас. д-р Иван Благоев
Експерт по кибер сигурност и партньор в ThinkCyber Bulgaria Ltd, оторизиран представител на израелската компания за кибер сигурност ThinkCyber Israel

Търсенето на експерти по киберсигурност се увеличава заедно с увеличаването на кибер атаките. Поради това се наблюдава широк интерес към курсовете за обучение в тази област. Фокусът на тези курсове е върху актуализирането на знанията, които трябва да се развиват изпреварващо спрямо рисковете и заплахите. Съществуват различни начини за предаване на знанията – от традиционните методи, базирани на лекции, до прилагане на активни методи, при които цялото обучение минава през практическото тестване.

Кибер полигонът като симулирана среда позволява да се извършват едновременно както обучения за ситуационни операции, така и тестове и изследвания с образователно развитие. Следователно кибер полигоните не са предназначени само за специализирани кибер организации и професионалисти (разработка, производство, поддържане), но имат за цел да подпомагат обучението на студенти и специалисти от различни организации / институции. Технологията, използвана за създаване на такива среди може да бъде фокусирана само върху хардуера, само върху софтуера или комбинация от двете. Тази среда е затворена и следователно безрискова (напълно контролирана от нас), което позволява осъществяването на сценарии от реалния живот, които не могат да се изпълнят в реална технологична среда и инфраструктура. Придобиването на практически умения, тестването на услуги или продукти, вкл. на тестове за сигурност са основните области на използване на кибер полигоните. Бъдещето на дигиталната трансформация и кибер устойчивите решения са пряко свързани не само с традиционни среди за обучение и тестване, но и с развитието на кибер полигоните. Макар кибер полигоните да са предназначени да покриват едни и същи цели, те се различават по възможности. Това се дължи на факта, че те се различават по мащаб и са базирани на различен технологичен подход при реализацията им, което води до различни по вид ограничения. Пример за това се наличните към момента основни видове инфраструктури на кибер полигони, а именно:

- **Частна инфраструктура:** Това са кибер полигони изградени на частна инфраструктура, които разполагат с изцяло частен хардуер под контрола на организацията. Това е сериозно предимство при провеждане на тестове върху системи, които трябва да оперират с чувствителни данни. В някои случай, чувствителните данни биха могли да се подменят с примерни такива, за да се защитят в среди, които не са под контрола на организацията. Но това не винаги е възможно, защото при някои видове тестове и анализ за кибер устойчивост, може да се прилага изкуствен интелект или друга функционалност, която ще реагира по различен начин в зависимост от съдържанието в данните. Същото е и при симулирани атаки чрез техники за социално инженерство, които отново се базират на данните и информацията. Съответно подмяната на данни не винаги е приложимо и би изкривило резултатите от тестовете и анализа от въздействие на симулирането на кибер атаките спрямо дадена среда. За това при наличие на тези фактори за тестваната система, ще се наложи използването на кибер полигон разположен върху частна инфраструктура. Частните инфраструктури дават повече възможности и за провеждане на различни видове кибер атаки, които в облачна инфраструктура биха били недопустими, защото могат изложат на риск функционирането на

облачната инфраструктура. Предимство е, че при планирането на разходите, за финансовите отдели частната инфраструктура е предвидима като разходи за напред във времето. Недостатък на този вид инфраструктурни решения е, че трудно се мащабират при необходимост от бързо разширяване за кратък период от време.

- **Публична инфраструктура:** Такива полигони са изградени върху публични облачни сървъри на различни доставчици на Virtual Private Server (VPS), като по-известни от тях са Amazon, Azure, Google и др. Недостатъците при използването на този вид инфраструктура са свързани с тестването на системи, използващи чувствителни данни, които ще се намират върху хардуер, който не е под контрола на организатора. Не е възможно да се провеждат тестове на някои кибер атаки (като DDoS, DNS Spoofing, MAC Spoofing и др.) поради ограничения за сигурност или защото могат да навредят на работата на облачната инфраструктура. Друг съществен недостатък е, че организацията трудно планира разходите по експлоатация на инфраструктурата за напред във времето. Като предимство се приема факта, че при необходимост бързо могат да се мащабират и да се поемат по-големи натоварвания извън планираните.
- **Хибридна инфраструктура:** Хибридните кибер полигони използват инфраструктура от смесен тип – и частна и публична. Този пип полигони се смята за един от много успешните варианти за инфраструктурни решения за кибер полигони, защото обединява предимствата и на двата вида и позволява да се планират и комбинират различните варианти в зависимост от поставената задача. При наличие на чувствителни данни, би могло данните да се разположат само върху частната инфраструктура. Няма ограничения за симулиране на различните видове кибер атаки в частната инфраструктура, а в същото време при необходимост от ресурси за различните симулации може да се използват предимствата на публичните облачни услуги.

Кибер полигон и симулатор – средства за обучение

Основен компонент за провеждане на обучения е симулаторът, който е връзката между задачите за обучаемите, техните действия и оценяването. Симулаторите могат да се интегрират със специализирани платформи за онлайн обучение, където да се съхраняват различни учебни материали, инструменти и др. При провеждане на обучение или изпит, действията на обучаемите се регистрират от симулатора и данните се събират за обработка от система за оценяване. Генерира се доклад с крайните резултати на обучаемите, който показва допуснатите грешки в теоретичен и/или практичен аспект. Предмет на оценка са основните елементи, като времето за решаване на задачата и броя на допуснатите грешки (CYBERIUM ARENA Simulator - THE ULTIMATE CYBER TRAINING TOOL).

При някой по-развити симулатори се допуска и повече от един начин за решаване на задачите, както и оценка за сложността на задачата, а от това се получава още една оценка за креативност/творчески подход.

На двете графики (Фиг. 1) се виждат в по-тъмен цвят средното ниво на допускане на грешки и времето за изпълнение от всички участници. С по-светъл цвят се вижда графиката на конкретния участник S3. Мисията, която е практически сценарий на тест за проникване в система и нейната защита, е изпълнена успешно. Действията по сложност на сканиране и проникване във виртуален сървър, разположен на полигона, са оценени в оранжевите правоъгълници.

Фиг. 1. Резултат от симулатор на академията ThinkCyber – Израел

Участникът е изпълнил задачата за 30 минути, получил е почти максимален брой точки 99.9 от 100, и е класиран на 1 място от общо 9 участника.

Методика за обучение

В повечето случаи популярната методика за обучение и изпит се подготвят от опитни експерти на принципа на академичните програми, където познавайки темите и материята по определена стъпаловидна последователност се изготвят материалите за обучение, упражненията и сложността на изпита. Всичко това чрез кибер симулатора е свързано с реална практика, като кибер полигоните позволяват наистина да се придобие опит за всички видове кибер заплахи. Подходът описан до тук е доказано ефективен и е един от най-често срещаните, но недостатък е, че се развива и поддържа от експерти, като винаги съществува известно забавяне от актуалните кибер заплахите на днешния ден в реалния свят и пресъздаването им от програмите за обучение често закъснява.

Академията по кибер сигурност ThinkCyber представя един по-различен и иновативен подход, който позволява обучението, упражненията и изпитите да са актуализирани съобразно кибер заплахите на реалния свят. Компанията е разработила ефективна система: Global Threat Analysis System, която функционира като „събирач“ на хакерски атаки (Worldwide Cyber Attack Collector) (Specto: Creating new scenarios on the Cyberium Arena Simulator). В реално време се наблюдават и регистрират кибер атаките по реални технологични инфраструктури. Тази система притежава сложна методика за анализ в реално време, която се подпомага и от изкуствен интелект, като успява да регистрира и защити системите, дори при едни от най-опасните атаки наречени нулев ден (Zero Day), срещу които производителите на софтуер не са разпространили все още съответните актуализации. В Академията по кибер сигурност ThinkCyber са направили връзка между Global Threat Analysis System и средствата за обучение, с цел да поддържат актуалност на обучение с текущи заплахи. Изпитните сценарии се базират на реални случаи на кибер атаки върху реална инфраструктура, но в условията на кибер полигон и симулатор на академията. Това позволява на системата за обучение да бъде възможно най-актуална спрямо съвременните заплахи и методите за тяхното откриване, за да подготвя едни от най-добрите експерти.

В ерата на продължаващата дигитална трансформация, кибер престъпленията са изключително значим фактор на заплаха срещу съвременните общества. Технологичният напредък е ключов за следващия

глобален скок в еволюцията и поради това необходимостта от кибер сигурност е осъзната, като се работи усилено за запълване на дефицита в сектора чрез развитие на кибер полигони, симулатори и обучението по кибер сигурност. Това е и една от основните цели на ЕДИХ – Тракия, където се създава среда – полигон и система за е-обучение/тестване/оценка, които да подпомагат развитието на компетентности и умения по кибер сигурност. Това ще подпомогне процеса на тестване и сертификация, оценка на зрелостта на системи/решения за киберсигурност, като се поддържа и акселерацията на иновации и консултирането в сферата на кибер устойчивостта. Изследват се редица концепции/реализации на кибер полигони и системи за обучение и оценка с цел проектиране на най-добрата за потребителите на ЕДИХ Тракия система, която ще бъде реализирана в края на проекта през 2025. Целта е до средата на 2024 да има проект на полигон със система за обучение и оценка, които отчитат натрупания опит от първите 18 месеца от традиционно обучение в ЕДИХ – Тракия, така че до средата на 2025 да има реализация с последващ тест през последните 6 месеца на кибер академия/CTEM център за ученици в сферата на киберсигурността.

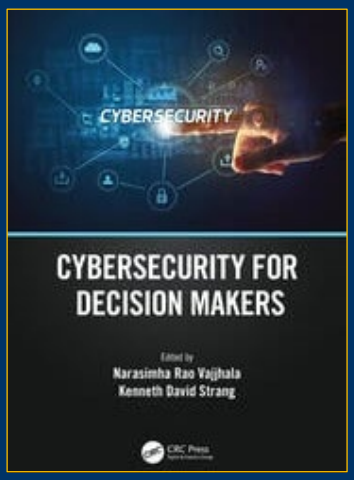
Кибер устойчивост по опита на NCI Academy

Официалното откриване на NCI Academy през септември 2019 г. предоставя на НАТО способност за обучение от световна класа, за да запази технологичното си предимство. NCI Academy предоставя обучение както по статични, така и по полеви/мобилни комуникационни и информационни системи на НАТО (CIS), въздушно командване и контрол (AirC2), киберсигурност и киберотбрана. В допълнение, академията играе ключова роля в проектирането и разработването на нови решения за обучение за клиенти, като извършва задълбочен анализ на нуждите от обучение и използването съвременни технологии за обучение.

Като акредитиран за осигуряване на качество център за образование и обучение на НАТО, NCI Academy се стреми към високи постижения чрез последователно прилагане на съответните политики на НАТО за обучение и стандарти за качество, за да постигне съгласувано предоставяне на услуги за образование и обучение.

Онлайн каталог за обучение в киберпространството на NCI Academy.

Книга: Cybersecurity for Decision Makers



Тази книга е насочена към лица, вземащи управленски решения, практици във всяка област и академичната общност. Авторите на главите са интегрирали теория с основана на доказателства практика, за да надхвърлят простото обяснение на темите за киберсигурността. За да постигнат това, редакторите използваха комбинираната когнитивна интелигентност на 46 учени от 11 страни, за да представят най-съвременното състояние на киберсигурността. Мениджъри и лидери на всички нива в организации по целия свят ще намерят обясненията и предложенията за полезни за разбиране на рисковете за киберсигурността, както и за формулиране на стратегии за смекчаване на бъдещи проблеми. Служителите ще намерят примерите и предупрежденията както за интересни, така и за практични за ежедневните дейности на работното място и в личния си живот. Практиците по киберсигурност в областта на компютърните науки, програмирането или шпионажа ще намерят

литературата и статистиката за очарователни и повече от вероятно потвърждение на собствените си открития и предположения. Правителствените политици ще намерят книгата ценна за информиране на новата им програма за защита на гражданите и инфраструктурата във всяка страна по света. Академични учени, професори, инструктори и студенти ще намерят теориите, моделите, рамките и дискусиите подходящи и подкрепящи преподаването, както и изследванията.

Някои от известните онлайн платформи за обучение по киберсигурност през 2023

Мъдростта на индустрията за киберсигурност препоръчва ученето на работното място като най-добрия начин за напредък в кариерата, като онлайн платформите са предпочитаният начин за получаване на сертификати. Това са някои от известните онлайн платформи за обучение по киберсигурност през 2023 г., безплатни и платени в зависимост от курса и други фактори:

- CISCO Netacad предлага безплатно сертифициране за киберсигурност. Курсовете могат да се използват от кандидати от различни сфери на живота, включително ученици от гимназията. Някои от курсовете са Въведение в киберсигурността, Дигитална грамотност, Програмиране, Интернет на нещата и Операционна система Linux. Студентите могат да се запишат в курсовете на предпочитания от тях език.
- Coursera предлага няколко безплатни и платени онлайн курса по киберсигурност от начинаещи до професионални нива. Платената сертификация за анализатор на киберсигурността на IBM, Certified Information Systems Security Professional (CISSP) струва $749, а Certified Information Systems Auditor (CISA) струва $575 за членове и $760 за нечленове са някои от тях. Coursera си сътрудничи с над 275 университета и компании като Google, Университета на Мичиган, AWS, Станфорд, Индийския технологичен институт в Бомбай, наред с други, за да предлага сертификати и курсове, предлагани от тях.
- edX предлага платени и безплатни сертификати за киберсигурност от компании като IBM и Check Point. Предлага висше образование, магистърска степен, бакалавърска степен и други. Могат да се избират курсове на над 53 езика в edX, предлага се табло за управление с анализ на данни почти в реално време, AR и VR, данни, които могат да се използват на място или в облака. Може също да се кандидатства за начални курсове по мрежова защита, етично хакване, дигитална криминалистика и т.н. от EC-Council, които са безплатни.
- Udemy е онлайн платформа за обучение по киберсигурност, предлагаща платени и безплатни сертификати за киберсигурност. Сред безплатните курсове са Amazon Web Services – Zero to Hero, Git & GitHub Course: Create a Repository from Scratch и др. Платените сертификати включват Total: CompTIA PenTest+, Complete Ethical Hacking Bootcamp 2023, Internet Security: A Hands-on Approach, Risk Management for Cybersecurity and IT Managers и др.
- CodeRed предлага обучение, базирано на абонамент, което често се избира от специалисти по киберсигурност. Повечето от учебните материали като видеоклипове и електронни книги са достъпни безплатно. Безплатното приложение може да се използва за достъп до материалите на курса.

- Pluralsight предлага видео обучение за разработка на софтуер, облачно инженерство, ИТ администратори и др. Организациите освен физическите лица могат да избират от разнообразието от налични курсове. За достъп до цялата библиотека хората могат да изберат план за плащане въз основа на техните нужди.
- Cybrary насърчава кандидатите в областта на киберсигурността със сертифициране по ИТ основи, анализ на злонамерен софтуер, реакция при инциденти, скриптове и т.н. Платформата предлага достъп до сертифициране, практическо обучение, виртуални лаборатории и т.н.
- HackTheBox предлага сертифициране на кандидати за хакерски и други курсове. Предлага демонстрация за фирми, която може да помогне на цяла група да се научи на по-добра киберхигиена, за да запази предприятието си безопасно.
- Simplilearn предлага онлайн сертификати за киберсигурност с виртуални стажове в известни мултинационални компании. Той предлага сертификати за киберсигурност въз основа на допустимостта и квалификацията на кандидата.
- upGrad подобно на други платформи, предлага както безплатни, така и платени курсове по киберсигурност онлайн. Твърдейки, че е предназначен за работещи професионалисти, upGrad предлага и възможности за работа.
- Microsoft предлага платени курсове по киберсигурност онлайн, в които можете да се запишете след полагане на основните изпити за допустимост според избрания курс по киберсигурност. Курсът Microsoft Cybersecurity Architect, наличен на множество езици, се таксува около $165.

Пълния текст на статията може да се прочете тук.

Посещение на Министърът на труда и социалната политика в обучителния център на ЕЦИХ „Тракия“

Д-Р ИВАНКА ШАЛАПАТОВА – МИНИСТЪР НА ТРУДА И СОЦИАЛНАТА ПОЛИТИКА: СЪТРУДНИЧЕСТВОТО НА МТСП СЪС СОЦИАЛНИТЕ ПАРТНЬОРИ Е ИЗКЛЮЧИТЕЛНО ВАЖНО

Министърът на труда и социалната политика посети обучителния център на Европейски цифров иновационен хъб „Тракия“ по покана на ръководството на Съюза за стопанска инициатива. Тя се срещна със студенти от Пловдивския университет и ученици 8-12 клас на училище „Паисий Хилендарски“ и Търговската гимназия в града, които в момента се обучават в кибер полигона на ЕЦИХ „Тракия“. ССИ е координатор на проекта, който се финансира по Програма "Цифрова Европа" на Европейската комисия и по Национална програма "Научни изследвания, иновации и цифровизация за интелигентна трансформация“.

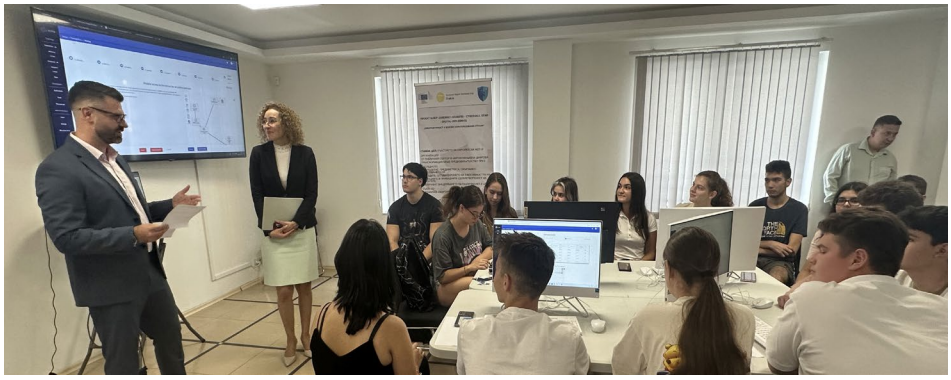
„Всички ние искаме държавата, общините и бизнесът ни да се модернизират. Заедно с развитието на дигитализацията стои и риска информацията много по-лесно да бъде компрометирана. Инвестицията в обучение и образование на младите хора е инвестиция в бъдещето. Фокусирането върху киберсигурността като стратегически приоритет е най-добрата превенция на риска, която можем да реализираме“, обобщи накратко Кузман Илиев – председател на ССИ.

Само половин година след стартирането на проекта над 600 души за преминали различни обучения, а успеваемостта им на изходните тестове е над 92%.

„Партньорството на МТСП със социалните партньори е изключително важно. България е на 26 място в Европейския съюз от гледна точка на индикатора за навлизане на информационните технологии в обществените среди. Повишаването на дигиталните компетенции е наш приоритет. Това, което виждам днес е много мотивиращо. Вашата мисия в ЕЦИХ „Тракия“ е голяма и вярвам в нея“, коментира д-р Иванка Шалапатова – министър на труда и социалната политика. Тя обяви, че близо 1 млрд. лв. ще бъдат инвестирани от тази година до 2026 г. именно в повишаване на дигиталните компетенции.

„Адмирирам широкото партньорство в сферата на киберсигурността, защото когато младите хора, местната власт и бизнеса са рамо до рамо - резултатите са налице“, добави министър Шалапатова.

„Щастливи сме,че сме част от екипа на ЕЦИХ „Тракия“. Вече около 30% от нашите служители са минали базовите обучения по киберсигурност. Партньорството е ключово в това направление. Сигурността е отборен спорт.“ Това коментира Мирослав Беляшки – началник отдел „Канцелария на кмета и протокол“, Община Пловдив.



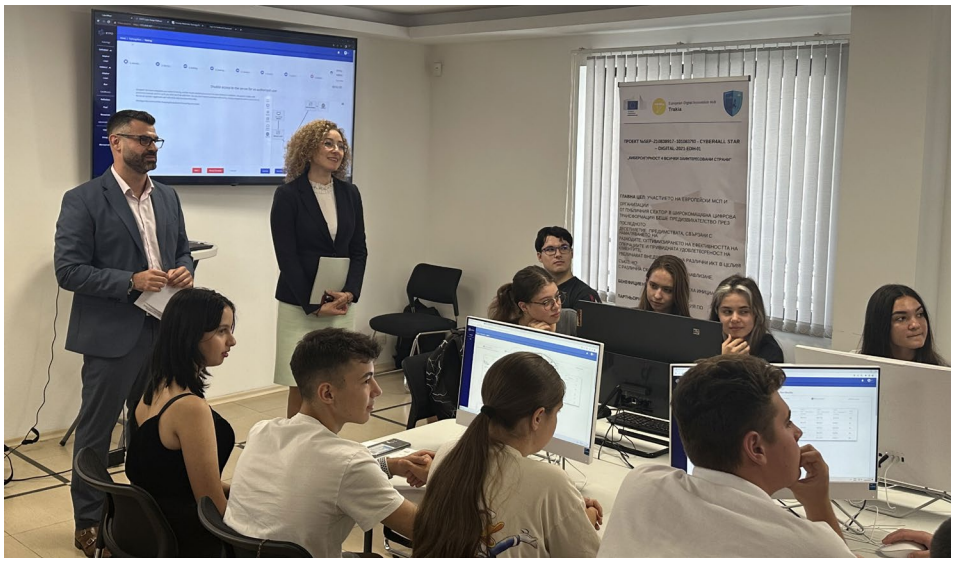
“Когато преди 4 години се събрахме да направим този проект, имахме 2 мечти. Едната беше да покажем, че европейски проект може да не бъде просто усвоен, а втората - да съберем тези експерти и те да върнат знанията си на обществото”, каза общинският председател на Съюза за стопанска инициатива в Пловдив Димитър Червенков. Той посочи, че основната цел на хъба е да предоставя технически и екосистемни услуги, достъп до инвестиране и обучения на служители и персонал. По думите му младежката програма не е била част от проекта, а е създадена, защото партньорите са искали да направят повече за обществото.

“Проведохме един експеримент. Решихме да видим колко деца се интересуват от киберсигурност. Показахме им базовите неща и след това ги питахме дали искат да се занимават с това. Сега вече имаме няколко групи от ученици”, заяви с гордост Червенков.

Светлин Илиев – председател на Българската асоциация по киберсигурност заяви, че широкото партньорство на ЕЦИХ „Тракия“ е спечелило доверието на Европейската комисия.

„Всички тези деца тук са нашите деца. И ние работим с мисъл и грижа за тях. Дигитализацията е нещо прекрасно, но заедно с нея трябва да развиваме и уменията си за защита в киберпространството“, завърши Светлин Илиев.

В рамките на посещението председателят на ССИ – Кузман Илиев и министър Иванка Шалапатова обсъдиха възможностите за сътрудничество между работодателската организация и МТСП в сферата на пазара на труда и липсата на работна ръка, преквалификацията на кадри и необходимостта от облекчаване на процедурите за легализация на дипломите на чуждестранните граждани.



Европейска организация за киберсигурност

Европейската организация за киберсигурност (ECSO) е създадена през 2016 като договорен партньор на ЕК за прилагане на уникалното публично-частно партньорство в Европа в киберсигурността – cPPP (2016-2020). Надграждайки успеха на cPPP, днес ECSO е уникална европейска междусекторна и независима членска организация за киберсигурност, която събира и представлява европейски публични и частни заинтересовани страни в киберсигурността и насърчава тяхното сътрудничество. Членовете на ECSO включват големи компании, МСП и стартиращи фирми, изследователски центрове, университети, крайни потребители и оператори на основни услуги, клъстери и асоциации, както и местни, регионални и национални публични администрации в държавите-членки на Европейския съюз и Европейска асоциация за свободна търговия.

Връзки към институции и инициативи

- DIGILIENCE 2023
- Cybersecurity@CEPS SUMMIT 2023: 6 December 2023
- ECSO's Annual CISO Meetup: 28-29 November 2023
- DTA
- ECSO
- Cyber Competence Network
- Cyberwatching.eu
- Съюз за стопанска инициатива
- ДИХ-Тракия
- Българска асоциация по киберсигурност
- ИИКТ-БАН
- ПУ „Паисий Хилендарски"
- Община Пловдив

Редакционен съвет

1. проф. д.н. Даниела Борисова – ИИКТ-БАН
2. доц. д-р Велизар Шаламанов – ИИКТ-БАН
3. Светлин Илиев – Цифров Иновационен хъб – Тракия, Българска асоциация за киберсигурност
4. проф. д-р Станимир Стоянов – Пловдивски университет „Паисий Хилендарски"
5. д-р Иван Благоев – ИИКТ-БАН
6. д-р Ирена Младенова –Софийски Университет „Св. Климент Охридски"
7. д-р Емилия Печева – Британско посолство в София

Публикуването на настоящия брой на бюлетина се реализира с финансовата подкрепа на проект: **#101083793 – CYBER4All STAR – DIGITAL-2021-EDIH-01 на ЕК**

British Embassy Sofia

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE

ПЛОВДИВСКИ УНИВЕРСИТЕТ 1961 ПАИСИЙ ХИЛЕНДАРСКИ

BCA BULGARIAN CYBERSECURITY ASSOCIATION
Българска асоциация по киберсигурност

ОБЩИНА ПЛОВДИВ