ISSN 2738-7089 https://doi.org/10.11610/cybsec10bg

Funded by the European Union

Digital Innovation Hub Trakia

ИИКТ
ИНСТИТУТ ПО ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ

Информационен бюлетин за киберсигурност

Бюлетин Декември 2023 Номер 10

Цели и обхват

Настоящия брой на информационния бюлетин за киберсигурност е фокусиран по темата на ransomware и средства за противодействие. Тази тематика присъства и в провежданите обучения от ЕЦИХ „Тракия“. В настоящия брой са представени най-често срещаните варианти на Ransomware. Описани са основните етапи на работа на Ransomware, като същевременно са обяснени и начините как да се предпазим и как да премахнем Ransomware

Представен е софуетърът Cybermira Anti-Ransomware, който използва иновативната технология Cyber Trap, създаваща виртуални околни среди и улавя зловредни софтуери чрез използването на „примамки“, предотвратявайки и спирайки ransomware атаки.

Отразен е проведения младежки кибер ден „Игра на хакове”, с участието на Петър Кънчев от ЕЦИХ „Тракия“, който провокираше участниците да създадат забавна, интересна и полезна игра за превенция на кибер заплахи по метода „Дизайн мислене“.

В изпълнение на своята мисия, ЕЦИХ „Тракия“ е в очакване на доставчици на иновативни напреднали технологии. Екосистемата на ЕЦИХ „Тракия“ е отворена за фирми-иноватори, които да се присъединят към нея. Първите фирми в екосистемата ще бъдат и пионерите във формирането на „Каталог на доставчиците на иновативни цифрови технологии“.

Представен е доклад на тема “Ransomware Landscape in Europe”, основно фокусиран върху Франция, Германия, Италия и Испания, който показва сериозно нарастване на атаките с ransomware, последвано от фишинг кампании. Освен статистически данни, докладът предоставя и насоки за прилагането на ефективни стратегии за киберсигурност, подчертавайки необходимостта от трансгранично сътрудничество в борбата с цифровите заплахи

В броя е представено скорошно изследване “Cybercrime and Businesses” от център за изследване на демокрацията, което дава поглед върху поведението на докладване, свързаните с това разходи и управлението на инциденти в България, Холандия и Испания.

Представен е форумът Securing Digital Future 21, както и някои конференции и конгреси по киберсигурност, планирани за 2024.

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

Съдържание:

Фокус на изданието:
Популярни варианти на Ransomware и как да се предпазим от него

доц. д-р Златогор Минчев, Главен мениджър по информационна сигурност в ИИКТ-БАН

Защо се появяват ransomware атаки? Съвременната лудост по ransomware започна с избухването на WannaCry през 2017 г. Тази широкомащабна и широко рекламирана атака показа, че атаките с ransomware са възможни и потенциално печеливши. Оттогава десетки варианти на ransomware са разработени и използвани в различни атаки. Пандемията от COVID-19 също допринесе за неотдавнашния скок на ransomware. Тъй като организациите бързо се ориентираха към дистанционна работа, възникнаха пропуски в тяхната кибер защита.

Популярни варианти на Ransomware

Съществуват десетки варианти на ransomware, всеки със своите уникални характеристики.

1. Ryuk е пример за много насочен вариант на ransomware. Обикновено се доставя чрез фишинг имейли или чрез използване на компрометирани потребителски идентификационни данни за влизане в корпоративни системи с помощта на протокола за отдалечен работен плот (RDP). След като системата бъде заразена, Ryuk криптира определени типове файлове (избягвайки тези от решаващо значение за работата на компютъра), след което представя искане за откуп. Ryuk е добре известен като един от най-скъпите съществуващи видове ransomware. Ryuk иска откупи, които са средно над 1 милион долара.

2. Ransomware Maze е известен с това, че е първият вариант на ransomware, който комбинира криптиране на файлове и кражба на данни. Когато мишените започнаха да отказват да плащат откупи, Maze започна да събира чувствителни данни от компютрите на жертвите, преди да ги шифрова. Ако исканията за откуп не бъдат изпълнени, тези данни ще бъдат публично изложени или продадени на предложилия най-висока цена.

3. Групата REvil (известна също като Sodinokibi) е друг вариант на ransomware, който е насочен към големи организации. REvil е едно от най-известните семейства ransomware в мрежата. Рускоезичната група REvil е отговорна за много големи пробиви като „Kaseya“ и „JBS“. През последните няколко години се състезава за титлата на най-скъпия вариант на ransomware, защото е известно, че REvil е поискал откуп от 800 000 долара.

4. LockBit е злонамерен софтуер за криптиране на данни, работещ от септември 2019 г. и скорошен Ransomware-as-a-Service (RaaS). Тази част от ransomware е разработена за бързо криптиране на данни в големи организации като начин за предотвратяване на бързото му откриване от устройства за сигурност и IT/SOC екипи.

5. DearCry. През март 2021 г. Microsoft пусна корекции за четири уязвимости в сървърите на Microsoft Exchange. DearCry е нов вариант на ransomware, предназначен да се възползва от четири наскоро

разкрити уязвимости в Microsoft Exchange. Ransomware DearCry криптира определени типове файлове.

6. Lapsus$ е южноамериканска банда за ransomware, която е свързана с кибератаки срещу някои високопоставени цели. Кибер бандата е известна с изнудване, като заплашва да разкрие чувствителна информация. Групата се похвали, че проникна в Nvidia, Samsung, Ubisoft и други. Те използват откраднат изходен код, за да прикрие файловете със зловреден софтуер като надеждни.

Представеният списък не може да бъде изчерпателен предвид постоянното развитие на областта и тенденцията за все по-висока интелигентност и автономност на ransomware решенията предвид високата им доходност.

Как работи Ransomware

За да бъде успешен, ransomware трябва да получи достъп до системата, да криптира файловете там и да поиска откуп от жертвата. Докато подробностите за внедряването варират от един вариант на ransomware до друг, всички споделят едни и същи основни три етапа:

Стъпка 1. *Вектори на инфекция и разпространение*. Ransomware, както всеки злонамерен софтуер, може да получи достъп до системите на организация по редица различни начини. Операторите на ransomware обаче са склонни да предпочитат няколко специфични вектора на инфекция, като един от тях са фишинг имейлите. Злонамереният имейл може да съдържа връзка към уебсайт, хостващ злонамерено изтегляне, или прикачен файл, който има вградена функция за изтегляне. Друг популярен вектор за заразяване с ransomware се възползва от услуги като протокола за отдалечен работен плот (RDP). Чрез RDP се да получава отдалечен достъп до компютъра в корпоративната мрежа и нападателят може директно да изпълни зловреден софтуер на машината. Повечето варианти на ransomware имат множество вектори на инфекция.

Стъпка 2. *Шифроване на данни*. След като ransomware получи достъп до дадена система, той може да започне да криптира нейните файлове. Някои варианти предприемат стъпки за изтриване на резервни копия и копия в сянка на файлове, за да направят възстановяването без ключа за дешифриране по-трудно. Други могат да се опитат да заразят системи директно, като например както WannaCry използва уязвимостта EternalBlue.

Стъпка 3. *Искане за откуп*. След като шифроването на файла приключи, ransomware е готов да поиска откуп, като не е необичайно фонът на дисплея да бъде променен на бележка за откуп или поставени текстови файлове във всяка шифрована директория с бележката за откуп. Ако откупът бъде платен, операторът на ransomware или ще предостави копие на частния ключ, използван за защита на ключа за симетрично криптиране, или копие на самия ключ за симетрично криптиране. Тази информация може да бъде въведена в програма за декриптиране (също предоставена от киберпрестъпника), която може да я използва, за да обърне криптирането и да възстанови достъпа до файловете на потребителя.

Днес все повече навлиза и асиметричното криптиране, където практически се дава достъп на потребителите до копие на техните данни, които след ransomware атаката могат дори да бъдат изтрити с цел гарантиране получаването на откупа, а услугата вече е факт и за поръчково външно изпълнение, като дори е възможно засегнатите да наемат хакерски групи, които да заличат техните данни. Всички заплащания стават анонимно посредством електронни валути (най-често „биткойн“ и се осъществяват в предимно в dark web) .

Тези три основни стъпки съществуват във всички варианти на ransomware, но различните ransomware могат да включват различни реализации или допълнителни стъпки. Например варианти на ransomware като Maze извършват сканиране на файлове, информация в регистъра и кражба на данни преди криптиране на данни, а WannaCry сканира за други уязвими устройства.

Как да се предпазим от Ransomware?

Възприемането на следните най-добри практики може да намали излагането на организация на ransomware и да сведе до минимум въздействието му:

Обучение и образование за информираност в киберпространството: Ransomware често се разпространява чрез фишинг имейли. Обучението на потребителите как да идентифицират и избягват потенциални атаки на ransomware е от решаващо значение. Тъй като много от настоящите кибератаки започват с насочен имейл, който дори не съдържа злонамерен софтуер, а само социално проектирано съобщение, което насърчава потребителя да кликне върху злонамерена връзка, обучението на потребителите често се счита за една от най-важните защити, които една организация може да разположи.

Непрекъснато архивиране на данни: Дефиницията на Ransomware казва, че това е злонамерен софтуер, предназначен да направи така, че плащането на откуп да е единственият начин за възстановяване на достъпа до криптираните данни. Автоматизираните, защитени резервни копия на данни позволяват на организацията да се възстанови от атака с минимална загуба на данни и без плащане на откуп. Поддържането на редовни резервни копия на данни като рутинен процес е много важна практика за предотвратяване на загуба на данни. Функционалните резервни копия също могат да помогнат на организациите да се възстановят от атаки на ransomware.

Корекция: Корекцията е критичен компонент в защитата срещу атаки на ransomware, тъй като киберпрестъпниците често ще търсят най-новите разкрити експлойти в наличните корекции и след това се насочват към системи, които все още не са с корекции. Като такова, от решаващо значение е организациите да гарантират, че всички системи имат най-новите корекции, приложени към тях, тъй като това намалява броя на потенциалните уязвимости в бизнеса, които атакуващият може да използва.

Удостоверяване на потребител: Достъпът до услуги като RDP с откраднати потребителски идентификационни данни е любима техника на нападателите на ransomware. Използването на силно удостоверяване на потребителя може да затрудни нападателя да използва позната или откраднатa парола.

Как да премахнем Ransomware?

Много успешни атаки с ransomware се откриват едва след като криптирането на данните приключи и на екрана на заразения компютър се покаже бележка за откуп. На този етап криптираните файлове вероятно не могат да бъдат възстановени, но някои стъпки трябва да бъдат предприети незабавно:

Поставяне на машината под карантина: Някои варианти на ransomware ще се опитат да се разпространят до свързани устройства и други машини. Ограничете разпространението на зловреден софтуер, като премахнете достъпа до други потенциални цели.

Оставете компютъра включен: Шифроването на файлове може да направи компютъра нестабилен и изключването на компютъра може да доведе до загуба на енергонезависима памет. Дръжте компютъра включен, за да увеличите максимално вероятността за възстановяване.

Създаване на резервно копие: Декриптирането на файлове за някои варианти на ransomware е възможно без плащане на откупа. Направете копие на криптирани файлове на преносими носители, в случай че решение стане налично в бъдеще или неуспешно усилие за декриптиране повреди файловете.

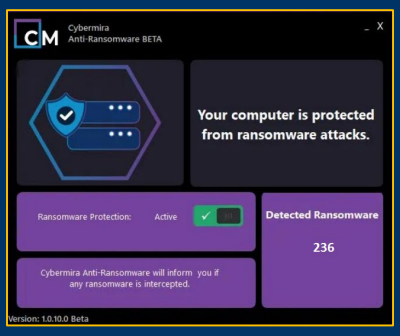
Проверете за декриптори: Проверете с No More Ransom Project, за да видите дали е наличен безплатен декриптор. Ако е така, стартирайте го върху копие на криптираните данни, за да видите дали може да възстанови файловете.

Поискайте помощ: Компютрите понякога съхраняват резервни копия на файловете, съхранени в тях и е възможно тези копия да бъдат възстанови, ако не са били изтрити от злонамерения софтуер.

Изтриване и възстановяване: Възстановете машината от чисто архивиране или инсталация на операционната система. Това гарантира, че зловредният софтуер е напълно премахнат.

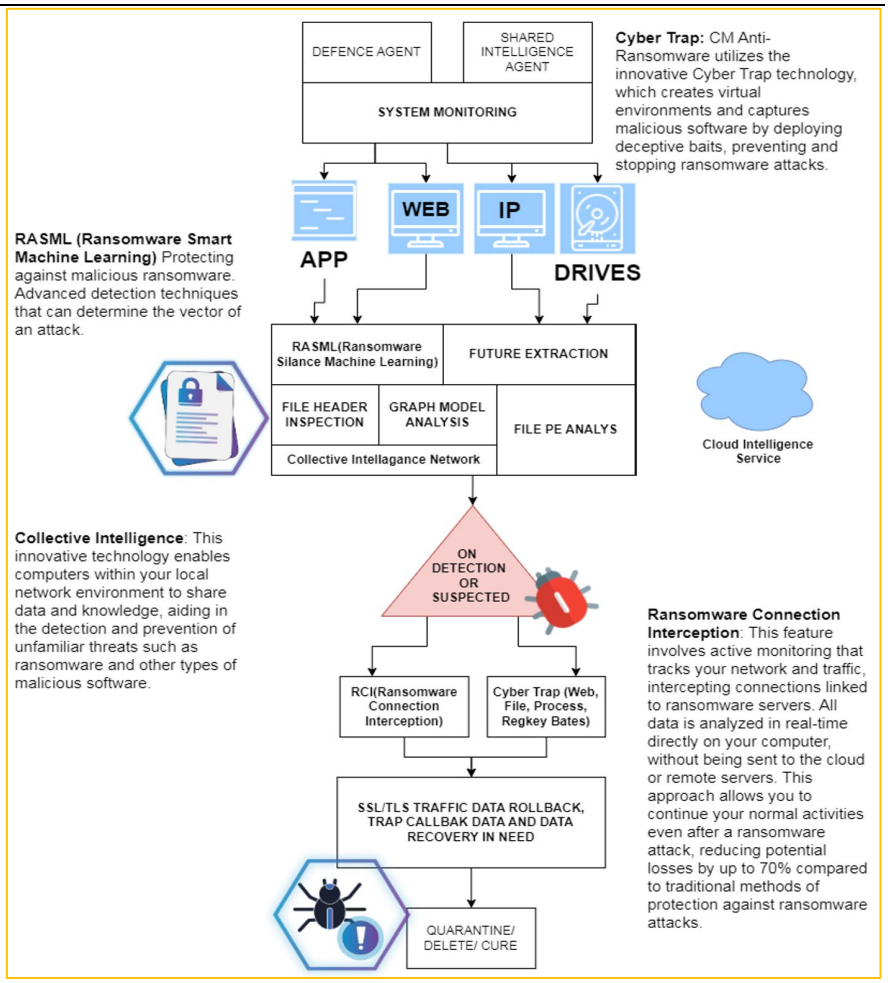
Пълният текст на статията може да прочетете **тук**.

Cybermira Anti-Ransomware



Cybermira Anti-Ransomware използва иновативната технология Cyber Trap, която създава виртуални околни среди и улавя зловредни софтуери чрез използването на примамки, предотвратявайки и спирайки ransomware атаки.

Cloud Intelligence: Cloud Intelligence технологията предоставя автоматичен анализ в реално време на потенциално зловредни файлове и незабавна реакция при засичане на заплахи. Използва се принципа на “honeypod” за създаване на примамки както в компютъра, така и в неговите процеси и услуги.



RASML: Защитава срещу зловреден ransomware, използвайки разширени интелигентни техники за проактивна детекция на векторите на атака.

Collective Intelligence: Тази иновативна технология позволява на компютрите в локалната мрежа да споделят данни и знания, което помага при засичането и спирането на непознати заплахи, като например ransomware и други видове зловреден софтуер.

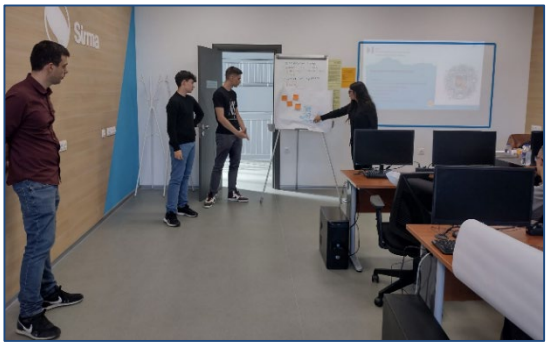
Ransomware Connection Interception: Тази функция представлява активен мониторинг, който следи вашата мрежа и трафика и прекъсва връзките, свързани с ransomware сървъри. Всички данни се анализират в реално време директно на вашия компютър, без изпращане в облак или на отдалечени сървъри. Този подход позволява да продължите нормалната си работа дори след ransomware атака, като намалявате потенциалните загуби с до 70% в сравнение с традиционните методи за защита срещу ransomware атаки.

Авторското, съвместно решение за противодействие на ransomware Cybermira Anti-Ransomware® е разработено съвместно с ИИКТ-БАН в рамките на инициативата Secure Digital Future 21 с участие на повече от 60 страни. Част изследванията и тенденциите за бъдещето в тази посока са отразени в отделна глава от книгата Digital Transformation in the Post-Information Age. Пълният текст на книгата може да бъде намерен тук.

Младежки кибер ден „Игра на хакове”

На 21.10.2023 се проведе младежки кибер ден „Игра на хакове”.

Ученици от 9. в и 12. в клас участваха в младежки кибер ден „Игра на хакове”. Събитието беше организирано от Европейски цифров иновационен хъб „Тракия“ в партньорство с Техническия университет – София, Министерството на образованието и науката, Българската асоциация по кирсигурност и други. Програмата на събитието включваше редица интересни и образователни теми, насочени към киберсигурността и възможностите пред младите хора за кариера в тази област. Участниците разгледаха техниките на социалното инженерство и предизвикателствата в цифровия свят свързани със защита на личните данни и информация. Учениците се включиха активно в хакатон „От играчка-плачка до играчка-пачка“.



Водещият на хакатона, Петър Кънчев от ЕЦИХ „Тракия“, провокираше участниците да създадат забавна, интересна и полезна игра за превенция на кибер заплахи по метода „Дизайн мислене“.

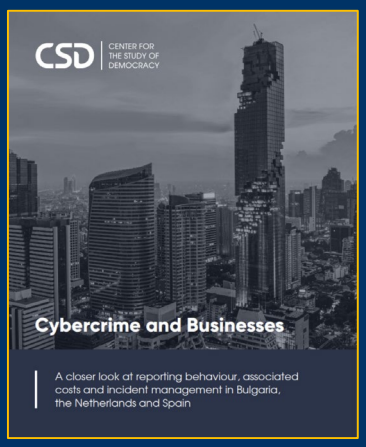
Основните аспекти върху, които беше насочено вниманието им бяха целите на играта и нейната аудитория, какви основни кибер заплахи ще се научат чрез нея и създаването на прототип на играта.

ЕЦИХ „Тракия“ в очакване на доставчици на иновативни напреднали технологии

Екосистемата на Европейски цифров иновационен хъб „Тракия“ вече е отворена и очаква фирми-иноватори да се присъединят към нея. Воден от стремежа си да развие и постави на високо ниво сътрудничеството между ангажираните в цифровия преход участници, Европейски цифров иновационен хъб „Тракия“ кани доставчиците на иновативни напреднали технологии да се присъединят към екосистемата на хъба. По този начин те ще бъдат пионери във формирането на „Каталог на доставчиците на иновативни цифрови технологии“ в изпълнение на проект „CYBERsecurity 4 All STAkeholdeRs“.

Заявка за включване в каталог на доставчиците на иновативни технологични продукти и услуги тук.

Изследване: “Cybercrime and Businesses”



“Cybercrime and Businesses” дава поглед върху поведението на докладване, свързаните с това разходи и управлението на инциденти в България, Холандия и Испания. То хвърля светлина върху докладващото поведение на бизнеса по отношение на инциденти с киберпрестъпления. Констатациите подчертават необходимостта от засилено сътрудничество между бизнеса и правоприлагащите органи, както и от подобрени системи за поддръжка за справяне с възприеманите ограничения на властите при разрешаването на инциденти с киберпрестъпления. Насърчаването на бизнеса да докладва за инциденти чрез кампании за повишаване на осведомеността и предоставянето на ресурси за вътрешно разрешаване на инциденти може да помогне за справяне с предпочитанията за вътрешно справяне с инциденти. Освен това усилията за обучение на бизнеса относно значението на докладването и потенциалните рискове, свързани с недостатъчно докладване, са от решаващо значение за ефективната борба с киберпрестъпността. Бизнесът, правоприлагащите органи, както и политиците трябва внимателно да обмислят тези фактори, когато формулират стратегии за справяне с недостатъчното докладване и насърчаване на по-устойчива и сигурна цифрова среда.

Пълният текст на проучването може да прочетете тук.

“Ransomware Landscape in Europe” кибератаките в Европа 2022 – 2023

57% скок на кибератаките в Европа, според доклада на DIGITAL SME. Основно фокусиран върху Франция, Германия, Италия и Испания, докладът показва сериозно нарастване на атаките с ransomware (от 112 през 2022 г. на 175 през 2023 г.), последвано от фишинг кампании, извършвани през същия годишен период. Разделена на общо четири тримесечия, текущата година се сблъска с постоянен пик на атаки още през Q1, където бяха публикувани 7772 нови често срещани уязвимости и експозиции (CVE), което още веднъж подчертава постоянно развиващия се и динамичен характер на кибернетичните уязвимости. Освен статистически данни и проценти, докладът предоставя и насоки за прилагането на ефективни стратегии за киберсигурност, подчертавайки необходимостта от трансгранично сътрудничество в борбата с цифровите заплахи.

Пълният текст на доклада може да прочетете тук.

Новини и събития по темата киберсигурност

Форумът Securing Digital Future 21 – SDF 21® стартира през 2017 г. с подкрепата на програмата на НАТО „Наука за мир и сигурност“, заедно с честването на 10-та на Съвместния център за обучение, симулации и анализ към ИИКТ-БАН. На фона на възхода на новите технологични и социални трансформации, идеята на форума съчетава изследователски и образователни усилия за устойчиво развитие на знанието в една доказана експертна общност. Днес форумът SDF21, обхваща повече от шестдесет страни, разпръснати по целия свят.

Повече за този форум може да прочетете тук.

Европейската комисия публикува поредица от нови покани за предложения по Програмата за цифрова Европа. Предоставя се специален бюджет от 84 милиона евро за дейности по внедряване в подкрепа на нови приложения на AI и други активиращи технологии за центрове за сигурност, прилагане на законодателството на ЕС за киберсигурност, като Закона за устойчивост на кибернетичното пространство, и европейския преход към пост-квантова криптография.

Повече за тази информация може да прочетете тук.

Връзки към конференции и конгреси по киберсигурност през 2024

- Gartner Identity & Access Management Summit – Лондон, UK (4-5 Март, 2024)
- EU Cyber Acts Conference – Брюксел, Белгия (11-13 Март 2024)
- Google Cloud Next '24 – Лас Вегас, NV, USA (9-11 Април 2024)
- Cybersecurity Expo – Бристол, UK (25 Април 2024); Манчестър, UK (24 Юли 2024)
- IOT Solutions World Congress – Барселона, Испания (21-23 Май 2024)
- CyberWiseCon – Вилнюс, Литва (23-24 Май 2024 & Online 20-21 Май 2024)
- Nordic IT Security Event – Стокхолм, Швеция (23 Май 2024)
- Cyber Security & Cloud Congress North America 2024 – Санта Клара, CA, USA (5-6 Юни 2024)
- AWS re:Inforce – Филаделфия, PA, USA (10-12 Юни 2024)
- it-sa Nürnberg 2024 – Нюрнберг, Германия (22-24 Октомври 2024)
- Critical Infrastructure Protection and Resilience Europe – Мадрид, Испания (12-14 Ноември 2024)

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