ЕВРОПЕЙСКИЯТ ЦИФРОВ ИНОВАЦИОНЕН ХЪБ ТРАКИЯ И ПРАВОТО НА (САМО)ЗАЩИТА В ДИГИТАЛНОТО ПРОСТРАНСТВО

Д-Р ХРИСТИАН ДАСКАЛОВ

Цифров иновационен хъб „Тракия“
h.daskalov@edihtrakia.org

Резюме: *Възприемайки подхода на координираното разкриване на уязвимости и създавайки съвременна правна рамка за етично хакерство, Европейският цифров иновационен хъб „Тракия“ застъпва тезата, че България може да допринесе значително за колективната киберсигурност на региона. Сигурността в киберпространството е не само индивидуална отговорност на местните власти или на малките и средни предприятия у нас, но и въпрос на международно сътрудничество и координация, за да може експерти по мрежова и информационна сигурност, обучени по проект Cyber4AllSTAR с подкрепата на ЕЦИХ Тракия да започнат да допринасят пълноценно за неутрализирането на киберзаплахи чрез етичното и координирано докладване на установени от тях уязвимости в активи, мрежи и информационни системи на трети страни, без риск от наказателно преследване по повод на изследователската работа, която се извършва в обществен интерес.*
Ключови думи: *киберсигурност, етично хакерство, координирано разкриване на уязвимости, цифров иновационен хъб Тракия, Cyber4AllSTAR проект.*

EUROPEAN DIGITAL INNOVATION HUB TRAKIA AND THE RIGHT OF SELF-DEFENSE IN THE DIGITAL SPACE

DR. HRISTIAN DASKALOV

Digital Innovation Hub Trakia
h.daskalov@edihtrakia.org

Abstract: *Adopting the approach of coordinated vulnerability disclosure and creating a modern legal framework for ethical hacking, the European Digital Innovation Hub "Trakia" advocates that Bulgaria can contribute significantly to the collective cyber security of the region. Cybersecurity is not only the individual responsibility of local authorities or small and medium-sized enterprises in the country, but also a matter of international cooperation and coordination, so that network and information security experts trained under the Cyber4AllSTAR project with the support of EDIH Trakia can begin to contribute fully to the neutralization of cyber threats through the ethical and coordinated reporting of vulnerabilities they identify in third-party assets, networks and information systems, without the risk of prosecution on the grounds of cybercrime.*
Key words: *cybersecurity, ethical hacking, coordinated vulnerability disclosure, digital innovation hub Trakia, Cyber4AllSTAR project.*

1. Въведение

В ерата на дигитализацията, където почти всички сфери на икономическия, обществения и личния живот са пряко свързани с киберпространството, необходимостта от сигурност и защита на цифровите системи става критично важна за всеки ръководител на средна или по-висока позиция, а оттам и обективната необходимост от осъзнаването на персоналната отговорност. Това ново измерение на защитата налага преосмисляне на концепцията за самоотбрана, която вече не се ограничава до физическото, а обхваща и цифровото пространство. Една от ключовите теми в това

отношение е „етичното хакерство“ и в частност - координираното разкриване на уязвимости (Coordinated Vulnerability Disclosure), които играят все по-голяма роля в глобалната киберсигурност. Това е тема, която Цифровият иновационен хъб „Тракия“ налага активно в общественото пространство на България, предоставяйки безвъзмездно технически и обучителни услуги за бизнеса в областта, с подкрепата на програма „Дигитална Европа“ на Европейската комисия и националната програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027 г. [1]

2. Етично хакерство и CVD

Етичното хакерство или изследването на кибер-уязвимости, се отнася до практиката, при която сертифицирани специалисти по киберсигурност (наричани разговорно "бели хакери") извършват тестове на мрежи и информационни системи, за да открият слабости и уязвимости, които биха могли да бъдат експлоатирани от злонамерени актьори в ущърб на собствениците и потребителите на тези системи. Тези тестове са правени с цел да се подобри сигурността на активите, като преди това се постигне договорното съгласие на собствениците им и се работи само в рамките на одобрени програми и планове за тестване. Етичните хакери следват международни стандарти и сертифицирани рамки, като по този начин гарантират, че техните действия не водят до щети или правни нарушения.

Координираното разкриване на уязвимости (CVD) е установен процес в основата на по-широкото изследване на уязвимости, който предоставя на етичните хакери и експертите по киберсигурност легитимен механизъм за докладване към собствениците на изследваните системи, а в определени случаи и към специализираните държавни органи по киберсигурността. В CVD процеса, когато „хакер“ открие уязвимост, той я свежда на вниманието на разработчиците или администраторите на съответната система (посредством възложителите на изследването), като предоставя информация за проблема и предлага решения за отстраняването му, но не участва в техническото им приложение. Този процес е ключов за изграждането на доверие между етичните хакери и организациите и се извършва по начин, който не поставя в риск сигурността на системата, компанията или държавата.

Проблемът идва оттам, че в общия случай, описан по-горе, договорното съгласие на собствениците на изследваните системи – било то от частния или публичен сектор, е единственият начин по който изследователите на кибер-уязвимости получават правна защита след като докладват отговорно разкритите уязвимости за последващо отстраняване. А данните за България са категорични – (почти) никой не желае външни експерти да обследват неговите системи, а настъпи ли инцидент – притаяването му е най-често срещаната тактика с цел избягване на административни и финансови главоболия. И така до следващия пробив…

3. Етичното хакерство като форма на анархия или обществено отговорен подход за (само)защита

Ако една компания за счетоводен софтуер стане жертва на кибер атака, това може да доведе до криптиране на компютърните системи на хиляди други фирми, използващи нейния софтуер. Т.нар. „атака по веригата на стойността“. Ако една държавна агенция не защити съхраняваните от нея потребителски данни, милиони могат да се озоват в уязвима ситуация при която личните им данни попадат в „тъмния интернет“ откъдето с години могат да се ползват за всевъзможни измами. Ако една обществена медия не обучи служителите си на базова кибер-хигиена, целият й архивен фонд може да бъде криптиран или изтрит в резултат на ransomware атака, заедно с резервните копия, което да унищожи културното наследство на една нация. Да изпратиш милиони на погрешния IBAN в резултат на социален инженеринг, може да фалира твоя бизнес за минути… Ето това е лицето на дигиталната анархия. И институционализирането на експертните усилия за ограничаването й не са заплаха, а възможност.

Досещате се, че посочените по-горе примери не са хипотетични, а са от съвременната българска практика. И въпреки тези примери, едва 7% от бизнесите разчитат на външна експертиза, която е от компании специализирани в областта на тестването за пробиви в киберсигурността и доставчици на този вид услуги за сигурност. Останалите над 90% следват принципа на мълчаливото заобикаляне на темата познат още като „don’t ask – don’t tell“ и разчитат изцяло на вътрешните си ресурси за преодоляване на предизвикателствата пред сигурността. Цитираните данни от актуално проучване за практиките в киберсигурността обхващат единствено български компании с персонал над 50 души и оборот над 50 000 лева. Процентът на търсещите услуги за активна сигурност става още по-нищожен ако се вземат предвид мнозинството микро и малки компании у нас, които олицетворяват феномена „кибер-

бедност“ – невъзможността да се отделят достатъчно инвестиции, за да се постигне базово ниво на киберсигурност, адекватно на международните стандарти.

Какъв е отговорът на държавата? В докладите за дейността на МВР и ДАНС през периода 2018 - 2023 г. се отчита висока честота на киберпрестъпления в България поради което се предприемат и необходимите мерки – реактивни и превантивни. За по-ефективно противодействие на нарастващите киберпрестъпления и на престъпните структури, използващи високотехнологични методи и средства, през март 2023 г. отдел „Киберпрестъпност” в ГДБОП-МВР е преструктуриран в самостоятелна дирекция, чиято дейност е насочена към борба с кибер- и киберсвързани престъпления, извършвани от организирани престъпни групи (ОПГ) и отделни лица, разкриване и документиране на престъпления, при които обект на нерегламентиран достъп са компютърни системи или мрежи, както и престъпления, чието извършване е практически невъзможно без кибер-пространството. Създаден е „Екип за реагиране при инциденти с компютърната сигурност“ на МВР, който поддържа готовност за координирана съвместна реакция с аналогичен национален екип към Министерството на електронното управление (МЕУ). Съвместно с партньори от гражданския сектор се организират превантивни кампании за образование, включващи лекции и презентации пред ученици и студенти.

Въпреки тези (и други) комплексни и споделени усилия на държавните власти, докладът за развитието на Интернет в България за 2024 г., изготвен по рамката на индикаторите за интернет универсалност на ЮНЕСКО, показва ръст на атаките и измамите, извършвани спрямо държавни институции, фирми и частни лица, свързани с използването на спам или т.нар. фишинг атаки, нерегламентиран достъп, кибератаки от типа „дистрибутиран отказ от услуга”, посредством използването на „бот-нет” мрежа, присвояването на акаунти в социалните мрежи, използването на т.нар. „ransomware” вирус и др. Зачестяват и кампаниите за дезинформация, създадени с цел умишлено разпространение на невярна информация. Все повече са сигналите, свързани с инвестиционни измами и неправомерен достъп до акаунти на лица, използващи интернет банкиране. Измамни сайтове за търговия стават инструмент за атаки, засягайки стотици български потребители. Обобщено, оценката на развитието на Интернет в България показва, че киберпрестъпленията в страната през последните години са в нарастваща тенденция, която засяга широк спектър от сектори и институции. Извършвани са различни видове нарушения, включително използване на зловреден код, спам, DDoS атаки, кражби на лични данни, финансови измами и разпространение на противоправно съдържание.

Заключението може да бъде само едно - подчертаната нужда от поддържане на високо ниво на информационна сигурност не може да се обезпечи само с институционалните усилия и ресурси на МЕУ, МВР и ДАНС, нито посредством отговорното поведение на сравнително малкия процент напредничави юридически лица от частния сектор, обръщащи се превантивно към корпоративните услуги на специализираните компании от сектор киберсигурност. Нещо повече – заключението за невъзможност за обезпечаване на нашата сигурност от страна на правителствените органи, която мисия следва да е фундамент на държавността, не е с регионални измерения. По оценка на „Statista“ през 2023 загубите от кибер атаки в глобален мащаб са били в размер на 8 трлн. долара. Прогнозата е, че до 2028 година атаките ще нараснат до 13,82 трлн. долара [2], което се равнява на настоящия брутен вътрешен продукт на Еврозоната. Ето защо са необходими допълнителни мерки за изграждане и активиране на капацитет в системата на киберсигурност като законовото регламентиране на дейността на изследователите на уязвимости в киберсигурността, т.нар. етични хакери.

4. Инкубаторите за „неетични хакери“

За да можем да се отбраняваме адекватно като общество в рамките на глобалните цифрови „бойни полета“, както и за да се самоотбраняваме ефективно от гледна точка на персоналната ни отговорност, ние следва да можем да се ползваме от правото да тестваме сигурността на системите, които избираме да ползваме като потребители или които сме заставени да използваме като граждани или като служители. Защото тези системи се тестват ежедневно, но от други „изследователи“ и с по-различни намерения.

Данните на Европейската агенция за киберсигурност (ENISA) и НАТО ясно показват, че една от основните заплахи за сигурността на цифровите системи в Европа и Северна Америка идва от пара-военните кибер-формирования, действащи в интерес на авторитарни режими. Например, групи като APT28 и Sandworm, свързани с руските разузнавателни служби, са известни със своите операции срещу западни правителства и инфраструктури, включително в България и други страни-членки на ЕС. Китайски

хакери като APT10 са специализирани в кражба на интелектуална собственост и корпоративни тайни, което нанася значителни щети на конкурентоспособността на европейските и американските компании. Това подчертава колко важно е да се изградят здрави правни рамки за координираното разкриване на уязвимости, за да може НАТО и ЕС да защитават своите членки и граждани от тези заплахи.

Координирана между партньорите децентрализирана отбранителна стратегия е необходима, за да се противодейства на държави като Северна Корея, която по актуални данни от скорошния „Euro-Resilience Forum“, провел се през м. октомври 2024 г. в Парламента на Букурещ, разполага с между 6 и 7 хиляди военни „изследователи“ на уязвимости в киберсигурността, чиято цел не е да докладват на МЕУ или МВР за тестваните от тях мрежи и системи, а да експлоатират и мултиплицират уязвимостите в тях. При това, тези данни обхващат само официално наетите в „кибер армията“ на Северна Корея, като не включват членовете на отделни престъпни синдикати и индивидуални кибер-престъпници. За последните две групи знаем, че също се ползват със защита от органите на вражески режими и често пъти демонстрират синергични „публично-частни партньорства“ с тях, когато „прогнилият либерален Запад“ следва да бъде уязвен.

Консервативните принципи винаги са подкрепяли правото на самоотбрана, но то трябва да бъде пропорционално и законово регулирано. Киберпространството не е изключение. Етичното хакерство и CVD представляват такива пропорционални мерки, които не нарушават принципите на закона и реда, но същевременно осигуряват възможност за ефективна самозащита. Докато международното законодателство и рамките на НАТО и ЕС се развиват в посока на създаване на повече правна сигурност за етичните хакери - доброволци, тези практики вече са изпитани като важен корпоративен инструмент в борбата срещу кибератаките, там където тестването на уязвимости се извършва по силата на договорна основа. Въпросът за установяването на социален контракт, който разширява приложното поле на защита отвъд лимитирания брой формални договори, не е лесен, но е необходимо да бъде решен. В България, за пример, едва веднъж държавата е организирала кампания за координирано разкриване и докладване на уязвимости, през 2023 г., при това с безкрайно ограничен периметър на действие. Фирмените „bounty“ програми, пък, при които компании предлагат възнаграждение на доброволци, които открият и докладват уязвимости в техните системи, се броят на пръстите на двете ръце.

Ако законодателството позволи на „етичните хакери“ да разкрият и да докладват уязвимости по координиран начин, без да се страхуват от юридически последствия, когато са действали без санкцията на собствениците на изследваните системи, Европа и нейните съюзници ще могат да поддържат по-здрава и гъвкава киберзащита, изградена отдолу-нагоре. Нещо повече, този допълнителен слой на защита ще може да намали щетите от вече настъпили инциденти чрез ранното им сигнализиране, доколкото тъкмо при държавно-спонсорираните кибератаки периодът между пробив и детекция е най-продължителен - може да надвиши 6-8 месеца. В България, като част от НАТО и ЕС, все повече ще се осъзнава нуждата от подобряване на киберсигурността чрез по-голяма прозрачност и координирано международно сътрудничество по темата, тъй като дори и да бъдат развързани ръцете на местните кибер-организации и сертифицирани експерти, огромна част от системите, които биха били тествани за уязвимости, са с международни измерения и правната защита на национално ниво няма да бъде достатъчна.

5. Възможността за законова реформа в България

Вече се изясни, че идеята за законово регулиране на CVD у нас отвъд случаите, обхванати от експлицитни договори, не е теоретична екзотика. За това, че евро-атлантическите партньори вече признават значимостта на етичното хакерство и CVD говори интензифицирането на различни пилотни правителствени и междуправителствени инициативи. За пример, на 30.10.2024 г. се състоя кръгла маса под егидата на Държавната агенция по киберсигурност на Румъния (DNSC) с участието на Европейския цифров иновационен хъб „Тракия“ (ЕЦИХ Тракия) и Българската асоциация по киберсигурност (БАК) от българска страна, която бе посветена точно на този въпрос. Румъния, която бе обект на канонада от руски кибератаки спрямо части от критичната инфраструктура на страната на по-ранен етап през годината, вече е поне две крачки пред България, имайки имплементирана политика за разкриване на уязвимости. В момента северните ни съседи работят и по уреждането на законовата защита на изследователите, които освен да докладват, следва да могат и да тестват за уязвимости без заплаха от преследване. В тази насока са указанията на Европейската агенция за мрежова и информационна сигурност /ENISA/ от

2023, която в свой скорошен доклад [3] препоръчва на страните членки, в навечерието на влизането в сила на NIS2 директивата за мрежова и информационна сигурност, да изградят такава законова рамка, която да предоставя закрила от съдебно преследване на изследователи на кибер-уязвимости, съблюдаващи съответните етични стандарти и установените CVD протоколи, въведени от Националните екипи за реагиране при инциденти във връзка с компютърната сигурност (НЕРИКС).

България, като член на ЕС и НАТО, има шанс да играе водеща роля в изработването на законодателство, което подкрепя и насърчава отговорното разкриване на уязвимости. Страната ни вече е въвела редица мерки за киберсигурност, но е необходимо по-нататъшно развитие на законовите рамки, които да позволяват на етичните хакери да действат свободно в рамките на ясни правила и без риск от правни последствия, стига да спазват принципите на CVD. Конкретното предложение на ЕЦИХ Тракия и БАК е НЕРИКС България към Министерството на електронното управление да стъпи на процедурата по етично и координирано докладване на уязвимости в киберсигурността, въведена през 2023 г. в Белгия, доколкото само преди броени седмици бе публикуван международният „Global Cybersecurity Index 2024“ [4], спрямо който Белгия, с резултат от 96.81/100, се нарежда сред водачите в глобалната киберсигурност. България, с общ резултат от 74.73, се нарежда в третото от пет нива на глобалната киберсигурност и отстъпва най-вече в сфери като мерките за изграждане на капацитет – област, която би била подпомогната най-силно от ангажирането на изследователите на уязвимости в киберсигурността при защитата на бизнеса и държавата от настъпване на кибер инциденти и намаляването на последиците от такива..

6. Заключение

От една по-различна консервативна гледна точка съществува опасението, че етичното хакерство може да се разглежда като форма на "взимане на закона в свои ръце", водещо до правна несигурност или дори до кибер-анархия. Понятието „кибер-милиции“ също се употребява от скептиците на правото да бъдем информирани за заплахите и да притежаваме уменията да ползване „оръжия“ за самоотбрана в цифровия свят. Тези страхове обаче не са оправдани, когато етичните хакери действат според ясно определени стандарти и рамки, каквито следва да бъдат заложени в националното и в международното право.

Така например, в белгийската практика, в рамките на процедурата по координирано докладване на уязвимости [5], авторите на CVD доклад не извършват престъпление по отношение на изясняването на фактите, необходими за доклада, при условие че са изпълнили четири важни условия. На първо място, следва да са действали без измамно намерение или намерение да причинят вреда. На второ място, следва да са уведомили за откриването на потенциална уязвимост организацията, отговорна за системата, процеса или контрола, възможно най-скоро и не по-късно от момента на докладването към НЕРИКС. На трето място, изследователите следва да не са действали извън това, което е било необходимо и пропорционално за проверка на съществуването на уязвимост. На четвърто място, етичните хакери следва да не са разкрили публично информацията, свързана с откритата уязвимост, не и без съгласието на НЕРИКС. Всяка друга възможна отговорност на докладващите лица, произтичаща от техни действия, които не са необходими за изпълнение на така описаната процедурата, продължава да се урежда от приложимото законодателство.

При отчитане на тези обстоятелства може да се направи заключението, че етичното хакерство е оправдан от идейна и практическа гледна точка подход за самоотбрана в киберпространството, при което целта е защитата на индивидуалната собственост срещу посегателства, но и на обществения интерес от злонамерени действия. Злоупотребата с неоткрити или неразкрити уязвимости в компютърни системи е един от основните начини, по които хакери, често действащи в интерес на враждебни държави или криминални организации, проникват в критични инфраструктури или корпоративни мрежи. Руски, китайски, севернокорейски и ирански хакерски групи (но не само) редовно атакуват правителствени агенции, корпорации и организации в страните-членки на НАТО и Европейския съюз. Тези атаки са част от хибридна война, целяща да подкопае икономическата и политическата стабилност на Запада, като същевременно събират интелектуална собственост или чувствителна за националната сигурност информация.

В подобни условия на глобална несигурност, етичното хакерство и в частност – CVD процедурите са не само легитимни, но и необходими компоненти на съвременната киберсигурност. Правото на самоотбрана в цифровото пространство трябва да бъде неразделна част от националната стратегия за

киберзащита, като бъде подкрепено със законодателство, което позволява на етичните хакери да изпълняват своята роля в защита на националните и корпоративни интереси на уязвимите организации. НАТО и ЕС продължават да имат ключова роля в глобалната киберсигурност, но е от съществено значение държавите-членки като България да вземат по-активно участие в създаването на правна рамка, която да улеснява процеса на координирано разкриване на уязвимости. Законодателството трябва ясно да разграничи етичните хакери от злонамерените актьори, като същевременно осигурява механизъм за безопасно и прозрачно докладване без страх от правни последствия за тези, които работят в интерес на киберсигурността. Само чрез подобни реформи можем да гарантираме, че и в цифровото пространство правото на самоотбрана ще бъде ефективно упражнявано в защита на националните интереси, икономическата стабилност и сигурността на гражданите на свободния свят.

ЛИТЕРАТУРА

1. European Commission. Cyber4AllSTAR project. Retried on October 226, 2024 from https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue/cyber4all-star
2. Statista. Analysis on the estimated cost of cybercrime worldwide 2018-2029. Retrieved on October 26, 2024 from https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
3. ENISA NIS Cooperation Group. Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies. Retrieved on October 26, 2024 from https://www.enisa.europa.eu/topics/vulnerability-disclosure
4. 2024 Global Cybersecurity Index. Online: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
5. Vulnerability Reporting to the CCB. Online: https://ccb.belgium.be/en/vulnerability-reporting-ccb