ISSN 2738-7089 https://doi.org/10.11610/cybsec02bg

British Embassy Sofia

Информационен бюлетин за киберсигурност

ИИКТ
Институт по информационни и комуникационни технологии

Британско-Българско партньорство в киберсигурността за МСП и организации

Бюлетин Август 2020 Номер 2

Цели и обхват

Съдържание:

Настоящият брой на бюлетина е фокусиран върху рисковете и предизвикателствата свързани със защитата на данните в ерата на COVID-19, поставяйки акцент върху динамиката на сигурността в киберпространството по време на първата вълна от затварянето вследствие на пандемията. Представени са допълнителни подробности за ефектите от изолацията, както и за приемливи и неприемливи очаквания за киберсигурността в близко бъдеще в условията на COVID-19. Очертани и дискутирани са и някои важни уточнения за дефинираната динамика в пейзажа на киберсигурността.

Разгледани са допълнителни акценти за бъдещите тенденции в защитата на данните, включително добавената стойност от класификацията на данните гарантираща повишена сигурност. Процесът може да се разглежда като подходящ за категоризация на данните. Това гарантира по-ефективното им използване и защита в корпоративните мрежи. В този контекст се предлага и решение за многослойно класифициране на данни от британската компания Boldon James, което е единствено по рода си. На следващо място, предотвратяването на загубата на данни, криптирането и управлението на правата са отбелязани като естествено продължение от гледна точка на регламентите на GDPR, акцентирайки върху DeviceLock EndPoint DLP Suite. Решението позволява цялостно управление на различните състояния на данните (rest, motion, transit, use) върху сложните архитектури в корпоративна среда.

Изданието запознава накратко читателя и с някои от водещите британски институции и инициативи в областта на сигурността и по-специално – Defence Science and Technology Laboratory (Dstl). Програмата за кибер системи на Dstl също е означена като неразделна част от междуправителствената трансформационна програма, предназначена да предостави високоефективни и еволюционни възможности за кибер защита на Обединеното кралство, осигурявайки по-голяма устойчивост на страната към кибер атаки.

От българска страна е анонсирана инициативата „Сигурност в дигиталното бъдеще 21" – световен изследователски форум, съчетаващ както научни, така и образователни усилия в доказана експертна общност с ценна партньорска подкрепа от почти 50 държави на петте континента.

Съюзът за стопанска инициатива (ССИ) е представен в този брой като един от водещите партньори в България за определяне на държавната политика, като същевременно запазва политическата си независимост. ССИ е национално представителна организация на работодателите от микро, малкия и средния бизнес. Има устойчиви интереси и партньорства през последните няколко години в областта на киберсигурността в индустриален аспект.

В по-приложната част от бюлетина са предложени практически препоръки за защита на данните и информацията за МСП и организации, заедно с последните кибер уязвимости споделени от водещи представители на индустрията като CISCO, Microsoft, Google, WordPress, Facebook, Autodesk и GNU/Linux. Накрая са приложени някои допълнителни връзки към български, британски и международни кибер институции.

Редактор на броя: **доц. д-р Златогор Минчев**

Фокус на изданието: Рискове и предизвикателства пред защитата на данните в ерата на COVID - 19

доц. д-р Златогор Минчев, ГМИС, ИИКТ-БАН, редактор на броя

В днешния свят, технологичният прогрес постоянно дооформя нашата реалност с нови интелигентни решения и услуги. Това от една страна придвижва обществото ни към ново ниво на тотална дигитализация, а от друга – отваря кутията на Пандора за невиждани рискове и предизвикателства пред сигурността. Последните комбинират триадата: хора, технологии и среда, които поради вътрешни и външни проблеми стават доста важни за самия трансформационен процес на смесената дигитална реалност от: хора, машини, биотоп и интелект. Трансформираната социална реалност на 2020 г., доминирана от пандемията с COVID-19, за първи път в историята на новия век поставя сигурността в положение, при което трябва да се справи с несигурната динамика на сблъсъците в технологичните, обществените и биологичните области, по доста непосредствен начин.

Следователно, много важно е да се отбележат три основни проблема, които трябва да бъдат проактивно решени от аналитичния екип на ГМИС:

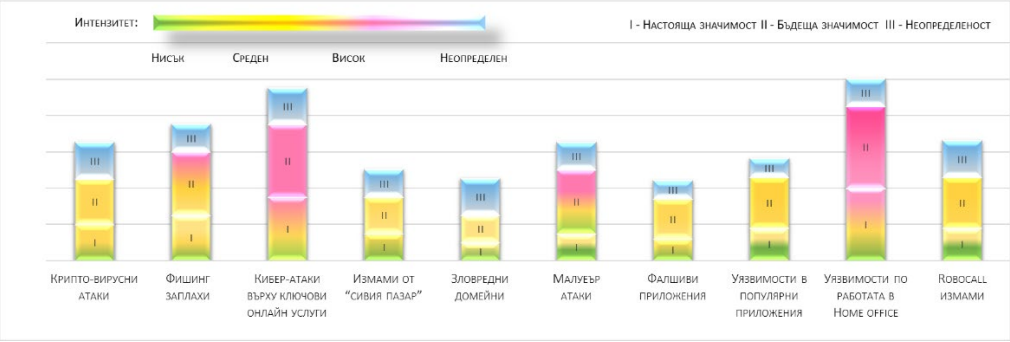
- Какви са предизвикателствата, рисковете и изводите за динамиката на сигурността в киберпространството по време на първата вълна от затварянето, вследствие на пандемията?
- Какви са ефектите върху киберсигурността след затварянето?
- Какви ще бъдат приемливите и неприемливите очаквания за киберсигурността в близко бъдеще, в условията на COVID-19?

Предвид факта, че анализа на тези проблеми е не само с информативен характер, но и ориентиран към реалната защитата на бизнес данните и информацията, по-нататък в изданието ще бъдат представени и някои полезни практически препоръки за тяхната защита.

Динамика на сигурността в киберпространството по време на първата вълна от COVID-19

Резултатите от първата вълна на COVID-19 с проактивна прогноза за 2020 г. могат да бъдат обобщени с „десет най-актуални социално-технологични рискове и заплахи“, анализирани в ИИКТ-БАН.

Приоритети се дават на атаките към ключови онлайн услуги и уязвимостите в наложилата се работна организация “Home Office”. Други важни акценти са фишинг заплахите и атаките със зловреден софтуер. Очаква се, но в по-малка степен и ръст по отношение на криптовирусни атаки, уязвимости в популярни приложения, robocall измами, фалшиви приложения и новини, измами от сивия пазар и злонамерени домейни.



Ефектите върху киберсигурността след COVID-19 затварянето

Освен проактивния характер на предварителните аналитични констатации за първата вълна на COVID-19, наскоро бяха наблюдавани и някои допълнителни обобщения, които заслужават да бъдат отбелязани:

- AI Enhanced Hybrid Threats – хибридни заплахи в смисъл на интелигентно взаимодействие между човек и машина, предназначени за генериране на фалшиви новини, фалшиви акаунти в социални мрежи, генериране на контакти и спам;

- Smart Infrastructure Attacks – свързани главно с IoT и отдалечено управляваните интелигентни домашни устройства, автомобили, камери, както и отнесени към суперкомпютърната инфраструктура.

Вдъхновението за тези атаки може да се обоснове с търсенето на икономически ползи, вследствие множеството негативни тенденции в целия свят, причинени от забавяне на икономиката и растеж на безработицата. Друга причина вероятно произтича от необходимостта за изява чрез хактивизъм на младото поколение, основно свързана с негативните социални ефекти и цялостните политически разногласия около изолирането по време на първата вълна на COVID-19.

Приемливи и неприемливи очаквания към киберсигурността за близкото бъдеще в условията на COVID-19

Да се прогнозират ефектите след COVID-19 затварянето е предизвикателство пред изследователската общност, защото те зависят от множество социални, биологични и технологични фактори. В този смисъл може да се очертае допълнително опростяване на някои приемливи и неприемливи очаквания, осигурявайки донякъде устойчиво управление на неопределеността в новата дигитална реалност:

Приемливи:

- Изтичания на данни;
- Уязвимости при въвеждане на хард- и софтуерните иновации;
- Компрометирани ресурси и Know-How.

Неприемливи:

- Кибер отмъщения и тероризъм;
- Скрит обмен на ресурси;
- Атаки, свързани със забавления.

В подкрепа на по-нататъшното разбиране на тези промени в сигурността на смесената дигитална реалност може да се вземат предвид: бъдещ растеж на компании в конкуренция за клиенти, причинени от негативните тенденции в развитието на социално-икономическата среда; устойчив интерес на потребителите към технологични иновации (включително множество нови услуги, приспособления и приложения); мотивация за бягство в паралелна и „по-цветна" дигитална реалност, която забавлява предимно младежите, демотивирани от потенциална бъдеща, нова социална изолация и цялостна трансформация на начина на живот.

Бъдещето в защитата на данните. Добри практики от Великобритания

Бъдещето в защитата на данните. Добри практики от Великобритания

Подсигуряването на новата дигитална ера е свързано и с ново ниво на защита на данните, което осигурява по-голяма защита на масивите от данни, по-силен регулаторен надзор и дори по-големи санкции за неспазване. Докато класификацията на данните предлага все по-убедителен отговор на въпросите относно неволното изтичане на данни, тя съвсем не спира до тук. По този начин ползите от ефективното категоризиране на данните далеч надхвърлят тяхната защитата.

Класификацията на данните е процес на организиране на данни в категории, подходящи за по-ефективно използване и защита в корпоративните мрежи. В контекста на защитата, данните се маркират въз основа на тяхното ниво на чувствителност, което улеснява намирането, проследяването и защитата според класа на чувствителност. По този начин класификацията на данните значително допринася за управлението на риска, спазването на нормативните изисквания и сигурността на данните.

За ефективно разработване на политика за класификация на данните категориите трябва да бъдат опростени, така че всички служители да могат правилно да ги прилагат. Въпреки, че те варират според нуждите на компаниите, обикновено се използват четири основни категории, когато става въпрос за чувствителни данни:

- Силно чувствителни данни – информация, която, ако бъде оповестена публично, излага компанията на опасност от

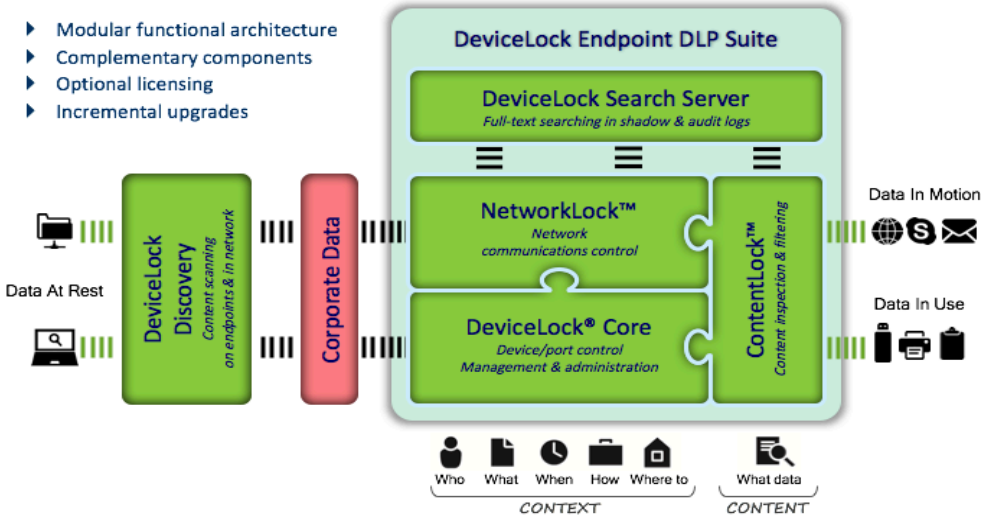
	юридически наказания, несъответствие с нормативните изисквания или финансови загуби. Това се отнася особено до личната идентификационна информация, също така и до фирмени записи и други категории данни, считани за чувствителни в зависимост от индустрията; • Вътрешни чувствителни данни – информация, която, ако бъде разкрита, може да представлява риск за дейността на компанията. Те включват данни за продажбите, информация за клиентите, заплати на служителите и т.н.; • Вътрешни данни – информация, която макар и да не е чувствителна, не е публично достъпна, като организационни схеми, маркетингови стратегии и други; • Публично достъпни данни – информация, до която всеки в и извън организацията има достъп, например, описания на продукти, адрес на фирма и т.н. Целта да се категоризират всички данни в дадена компания е разумна, но малко компании могат да си я позволят. Като се имат предвид огромните количества данни, които организациите в момента обработват, съвсем естествено е маркирането на всяка единица от данни да е тромаво, отнемащо време и в крайна сметка скъпо начинание. Следователно, от съществено значение е компаниите да изградят свои собствени категории за класификация на данните, които включват както чувствителни данни, дефинирани от различни регламенти, с които са длъжни да се съобразяват, така и чувствителни данни, които се считат за специфични за отрасъла. Улесняването на намирането на чувствителните данни от обработващия лични данни е от съществено значение, съгласно новите разпоредби като GDPR, които изискват от компаниите не само да могат да намират такива данни и да ги защитават, но и да демонстрират капацитета си за обработка. Също така е важно организациите да изпълняват исканията на потребителите за достъп или изтриване на личните им данни в рамките на определен период от време. Неизпълнението на тези задачи може да доведе до големи санкции и загуба на доверието на клиентите. Класификацията на данните повишава стойността и ефикасността на цялостната информационна сигурност и екосистемата за управление на данни. Трябва да се отбележи, че се добавят нови нива на интелигентност към решенията за архивиране и предотвратяване на загубата на данни. Всичко това стимулира по-високите нива на възвръщаемост при инвестиции в защита на данните. И най-накрая класификацията на данните позволява по-лесно и последователно прилагане на контролите, правилата и политиките за сигурност.
Какво представлява класификацията на данни?	Класификацията на данните е от основно значение за защитата и управлението на данните, но може да направи много повече за подсигуряването на бизнеса. Основната причина, поради която повечето организации се насочват към класифициране на създаваните и обработваните от тях данни, е за да контролират достъпа до чувствителна информация, водени от необходимостта да управляват риска за сигурността и да се съобразят с разпоредби, като например GDPR. Този обхват на целите, обаче е твърде тесен. Като се фокусират единствено върху тези цели, те пропускат възможността да наблегнат върху категоризацията на данните и да извлекат по-голяма бизнес стойност от всичките си информационни активи.
Класификация на данни и разпоредби	Всички организации трябва да спазват правилата на своите индустриални органи и на държавите, в които оперират. Постигането на съответствие е сложно. Налични са безброй инструменти за подпомагане на защитата и контрола на данните, вариращи от единични продукти до цели интегрирани системи. Всичко това консумира бюджетите за капиталови и оперативни разходи. И така, каква е ползата от цялата тази инвестиция? Евентуалното намаляване размера на санкциите в резултат на неспазване на изискванията, това със сигурност е похвална цел, но трябва да има по-добри причини от тази, за да се инвестира.

Нараства тенденцията клиентите на класифицирани данни да задават по-широки въпроси относно своята информация. Те възприемат тази перспектива на проблема, като преминават от начина на мислене: „ние разполагаме с всички тези данни – трябва да ги защитим", към „ние имаме всички тези данни – искаме те да работят по-твърдо за нас". За да идентифицираме допълнителни ползи от контрола на данните, трябва да погледнем отвъд простото спазване на правилата и управлението, и да се съсредоточим върху бизнеса – какво прави, къде го прави и как го прави – да разкрием информационните активи, които са в основата на всички бизнес процеси. Инструментите и подходите, използвани за постигане на съответствие, имат много по-широка роля в предприятието, като помагат за извличането на максимална стойност от тези информационни активи.

Многослоен подход за сигурност

Решения за класификация на данни, като UK Boldon James Classifier попълват празнината между по-традиционните решения за ИТ сигурност (като защитна стена) и решенията за управление на информацията. Все по-често класификацията на данните се превръща в част от най-добрите практики в многослойния подход за сигурност, който може да включва предотвратяване на загуба на данни, криптиране и управление на права. След като данните са класифицирани по подходящ начин, различните инструменти за защита като: DeviceLock EndPoint DLP Suite; криптиране на електронна поща, базирано на политики за сигурност или инструменти за контрол на достъпа и управление на данни, са експоненциално по-ефективни, тъй като те имат достъп до информацията, предоставена от етикета за класификация и метаданните, които им казват как трябва да се управляват и защитават данните.

Много организации са инвестирали в технологии за сигурност, от които тепърва трябва да извличат ползите на които са се надявали, или които са им били обещани. Добър пример е решение за предотвратяване на загуба на данни (DLP). Организациите, използващи този тип решения, често изпитват неудовлетвореност заради лошото възприемане от крайния потребител, претоварването на системите за управление на събития и постоянната нужда от прецизиране на политиките и правилата. Когато данните са класифицирани от потребителите, които разбират контекста им, чрез прилагането на метаданни в съобщението или файла, инструментите за предотвратяване на загуба на данни могат да използват тази допълнителна контекстна информация, за да осигурят по-ефективни резултати, с по-малко грешки, подобрен потребителски опит и по-голямо общо намаляване на риска.



Кибер институции и инициативи във Великобритания и България

Defence Science and Technology Laboratory (Dstl)

Defence Science and Technology Laboratory (Dstl) е изпълнителна агенция на Министерството на отбраната на Обединеното кралство, която работи по търговски линии. Това е една от основните правителствени организации, посветени на науката и технологиите в областта на отбраната и сигурността. Създадена е през 2001 г., след разцепването на Defence Evaluation and Research Agency (DERA). Първоначално, Dstl се занимава с научни и технологични дейности, които най-добре се извършват в рамките на правителството, докато индустриалната дейност на DERA е прехвърлена на държавната компания Qinetiq. През 2018 Dstl погълна Home Office's Centre for Applied Science and Technology (CAST), като пое ангажимента за прилагане на науката и технологиите в подкрепа на операциите на CAST за доставка на първа линия и предоставяне на доказателства в подкрепа на политиката и изпълнението на определени регулаторни функции. В момента Dstl е доказан национален актив, давайки на Обединеното кралство явно предимство в областта на науката, технологиите, киберпространството и информацията.

Програма за кибер системи на Dstl

Програмата за кибер системи на Dstl е неразделна част от междуправителствената програма за трансформация, предназначена да осигури високоефективни и еволюиращи възможности за кибер защита на Обединеното кралство, като гарантира, че Обединеното кралство е по-устойчиво на кибер атаки и може да използва възможностите на киберпространството.

По-конкретно, програмата е ангажирана с:

- принос към кибер политиката чрез предоставяне на научно-технически съвети;
- оценяване на придобиването на продукти и услуги за кибер отбрана от индустрията, като поддържа суверенна способност за разследване на уязвимости в киберпространството, за да защити платформите, системите и инфраструктурата от кибер атака;
- разработване на нови похвати и методи за визуализация, засичане, обработване и точно предаване на информация за действителното или вероятно реално въздействие на събитията в киберпространството.

Инициативата „Сигурност в дигиталното бъдеще 21“

Инициативата **„Сигурност в дигиталното бъдеще 21“** е формирана през 2017 г. с подкрепата на програмата на НАТО „Наука за мир и сигурност“ като последващо устойчиво общностно развитие и във връзка с отбелязването на 10-годишнината от основаването на Съвместния център по обучение, симулация и анализ към ИИКТ-БАН.

Създадена в началото на нова технологична и социална революционна трансформация, идеята за форума комбинира научноизследователски и образователни усилия в устойчив капацитет на знанието за една доказана експертна общност с ценна партньорска подкрепа от почти 50 държави на петте континента.

Основната цел е да се създаде дигитален уеб портал за обмен на експертни и изследователски мисли, иновации и виждания по отношение на новата кибер-физическа трансформираща се екосистема, обхващаща технологии, знания, хора и саморазвиващ се изкуствен интелект за успешното изграждане на бъдещото дигитално общество.

По този начин основателите вярват, че ще могат да се разберат по-добре бъдещите трансцендентални дигитални ефекти на новата трансформация и ще се подготви обществото за успешното посрещане на предстоящите преки и косвени промени в сигурността.

Съюз за стопанска инициатива

Съюзът за стопанска инициатива (ССИ) е национално признато сдружение на работодателите в България. В своята 30-годишна история ССИ се утвърди като един от водещите партньори на държавата при разработването на политики. Членовете на ССИ са предимно представители на малките, средните и микро предприятията.

През 2018 г. ССИ стартира инициатива за изграждане на общност, фокусирана върху нововъзникващи технологии и киберсигурност, като по този начин се превърна във важен партньор на дигиталната общност в България. От тогава съюзът привлече като членове и близки сътрудници Българската асоциация за киберсигурност, Асоциацията на сертифицираните етични хакери, Българско дрон общество, Български клъстер за изкуствен интелект, Европейски институт по киберсигурност, Институт за високи технологии в индустрия 4.0 и много други. Като национална работодателска организация, ССИ е част от процеса на разработване на политики в България чрез участието си в Тристранния диалог между държавата, бизнеса и синдикалните организации.

От 2019 г. ССИ е активен член на Европейската организация за киберсигурност, като през 2020 г. двете организации подписаха споразумение за участие инициативата „Cyber security made in Europe“. Също така, през 2020 г. ССИ и ИИКТ-БАН подписаха меморандум за сътрудничество. Общата цел на двете организации е да улеснят процеса на сигурна дигитализация на българските МСП и организации.

Десет практически препоръки за защита на данните и информацията към МСП и организации

Постигането на успешна защита на данните и информацията в новата трансформирана дигитална реалност, повлияна от пандемичните социално-технологични предизвикателства и рискове от COVID-19, е сложна и динамична задача, решаването на която съчетава както машинен, така и човешки интелект. Акцент може да се постави на десет избрани мерки за защита, както следва:

- Прилагане на системи за предварителна класификация на данните за определяне на подходящ дигитален пейзаж от данни, хора и устройства за по-нататъшно цялостно осигуряване;
- Внедряване на клауд базирани или самостоятелни, редовно обновяващи се антивирусни защитни платформи (включително и за мобилните устройства) с добро анти-спам и анти-фишинг филтриране, надеждни архивиращи системи (както на сървъри, така и на преносими устройства);

	• Периодично администриране на сигурността и актуализация на базовия и системен софтуер, включително подходящо „закърпване" и устойчиво архивиране; • Ефективна конфигурация и внедряване на системи за разузнаване на заплахи, системи за откриване на проникванията, системи за предотвратяване на проникване, предотвратяване на загуба на данни, управление на пароли и защитни стени; • Решения за управление на непрекъснатостта на работата и използване на системи и процедури за възстановяване при аварии; • Стратегии за управление на риска с разработване на съответни политики за сигурност и прилагане на подходящ външен достъп до корпоративни ресурси чрез защитени виртуални частни мрежи за отдалечен достъп; • Редовно обучение с иновации за повишаване на осведомеността относно сигурността и кибер хигиената, приемайки световно доказани най-добри практики за безопасна работа с данни и информация; • Повишен контрол на достъпа и обмена на данни и информация за акаунти в социални мрежи, клауд услуги за игри и външни интелигентни устройства с автономна мрежова свързаност, включително нерегистрирани преносими памети в офис среда; • Потвърждаване на технологичните решения, репутацията и произхода на доставчиците на услуги; • Избягване внедряването на продукти, решения и услуги на трети страни (или тези от сивия пазар), върху важни компютърни конфигурации, мобилни платформи и частни мрежи.
	Избрани новини за последните кибер уязвимости
Доклад на INTERPOL показва тревожен процент на COVID-19 кибер атаки	Доклад на INTERPOL, оценяващ въздействието на COVID-19 върху кибер престъпността, разкрива значителна промяна на целевите мишени – от физически лица и малък бизнес към големи корпорации, правителства и критични инфраструктури. Тъй като организациите и фирмите бързо внедряват системи и мрежи за отдалечена работа за да помогнат на персонала да работи от вкъщи, престъпниците също се възползват от увеличените уязвимости в сигурността за да крадат данни, да генерират печалби и да причиняват пробиви. Основни констатации, подчертани от оценката на INTERPOL за кибер престъпността във връзка с пандемията COVID-19, включват онлайн измами, Phishing, Ransomware, DDoS, Data Harvesting Malware, Malicious Domains и дезинформация. Източник INTERPOL …
Новооткрита уязвимост "BootHole"	Новооткрита уязвимост (CVE-2020-10713), наречена „BootHole" в програмата за начално зареждане GRUB2, заплашва милиарди устройства с Linux и Windows, позволявайки на нападателите да пречат на процеса на зареждане, предшестващ стартирането на операционните системи и потенциално да получат пълен контрол над системите. Източник ZDNet …
Уязвимости на Cisco Small Business Switches & Products	Cisco очертава над 60 нови уязвимости в Cisco Small Business Switches, Webex meeting, камерите и други техни софтуерни решения. Сред тях са около 20 сериозни заплахи и 2 критични – адресиращи инфраструктурния софтуер на Cisco Enterprise NFV и отдалеченото изпълнение на код, отказ от услуги (DoS) или разкриване на информация. Източник Cisco…
Уязвимост на браузъра Google Chrome	Уязвимостта на браузъра Google Chrome (CVE-2020-6519) позволява на нападателите да заобикалят политиката за сигурност на съдържанието на уебсайтовете, за да крадат данни и да изпълняват измамен код при милиарди потребители. Източник Threat Post…
Microsoft August 2020 Patch поправя 120 уязвимости	През м. август, 2020 от Microsoft са поправили 120 уязвимости в 13 различни продукта, от Edge до Windows и от SQL Server до NET Framework. Сред отстранените 120 уязвимости, 17 грешки са получили

	най-високата степен на класификация „критично“. Установени са и две атаки от типа “zero days”, които са били използвани от хакери, преди Microsoft да може да предостави новите корекции. Източник ZDNet…
WordPress Facebook компрометиращ Plug-in	Грешка с висока степен на сериозност, открита в официалния плъгин за чат на Facebook за уеб сайтове на WordPress, позволяваща на нападателите да прихващат съобщения, изпратени от посетители до собственика на уязвимите сайтове. Източник Bleeping Computer…
Хакери експлоатират недостатък в Autodesk при скорошна атака, част от кибер шпионаж	Злонамерени субекти използваха уязвимост в популярния софтуер за 3D компютърна графика Autodesk, за да предприемат неотдавнашна кибер шпионска атака срещу международна компания за архитектурно и видео производство. Изследователите казват, че по-нататъшният анализ на атаката сочи към сложен тип APT проникваща група. Атакуващите са имали предварителни познания за системите за сигурност на компанията и използваните софтуерни приложения, което е позволило внимателно планиране на атаката за проникване в компанията и разкриването на нейни данни. Известно е, че целевата компания, която изследователите не са посочили, е сътрудничила в милиардни проекти за недвижими имоти в Ню Йорк, Лондон, Австралия и Оман. Източник Threat Post …

Връзки към кибер институции

Връзки към български, британски и международни органи	• Сигурност в дигиталното бъдеще 21, Световен икономически форум • DSTL, DSTL програма за кибер системи - Великобритания • Институт Ponemon, Интерпол • (ISC)², Paloaltonetworks, Съюз за стопанска инициатива

Обратна връзка

За въпроси и препоръки	E-mail: acerta@bas.bg

Редакционен съвет

Академична CERT (ACERTA) организация съгласно споразумение, подписано от група академични органи (ИИКТ, ИО-МО, ЕСИ-ЦИЕ, като начало), за засилване на сътрудничеството в изследванията, свързани с киберсигурността	1. доц. д-р Велизар Шаламанов – зам. Директор на ИИКТ-БАН 2. проф. д-р Тодор Тагарев – ИИКТ-БАН 3. проф. д.н. Даниела Борисова – ГИМ, ИИКТ-БАН 4. доц. д-р Златогор Минчев – ГМИС, ИИКТ-БАН 5. полк. доц. д-р Николай Стоянов – зам. Директор на Института по отбрана към МО 6. д-р Георги Шарков – управител на фондация Европейски софтуерен институт – Център Източна Европа 7. Светлин Илиев – Съюз за стопанска инициатива

Публикуването на бюлетина се реализира с финансовата подкрепа на Британското посолство в София.

Бюлетинът отразява гледната точка на авторите.

British Embassy Sofia

ИИКТ Институт по информационни и комуникационни технологии

Институт по отбрана - МО

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE

DIGILIENCE Conference Series https://digilience.org