IT4Sec Reports 143
http://dx.doi.org/10.11610/it4sec.0143

Ниво на зрялост на кибер сигурността на инфраструктурата в домейна iict.bas.bg

Велизар Шаламанов, Иван Благоев, Илиян Илиев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, декември 2021

Велизар Шаламанов, Иван Благоев, Илиян Илиев, Ниво на зрялост на кибер сигурността на инфраструктурата в домейна iict.bas.bg**,** *IT4Sec Reports 143* (декември 2021), http://dx.doi.org/10.11610/it4sec.0143

IT4Sec Reports 143 „Ниво на зрялост на кибер сигурността на инфраструктурата в домейна iict.bas.bg“ Описание на нивото на зрялост на ИТ инфраструктура за домейн iict.bas.bg.

Ключови думи: кибер сигурност, криптография, сигурност, защитна стена, FTP, E-Mail, уеб услуги

IT4SecReports 143 „Level of maturity of the Cybersecurity of the infrastructure in the domain iict.bas.bg“ Description of the level of maturity of the IT infrastructure for the domain iict.bas.bg.

Keywords: cyber security, cryptography, security, firewall, FTP, E-Mail, web services

ISSN 1314-5614

УВОД: ЦИФРОВА ТРАНСФОРМАЦИЯ И КИБЕРУСТОЙЧИВОСТ НА ИИКТ-БАН - Е-ИНФРАСТРУКТУРА И СИГУРНОСТ. 4

1. СВЪРЗАНОСТ НА УСЛУГИТЕ КЪМ ДОМЕЙНА IICT.BAS.BG 5

2. СЪРВЪР ОТГОВАРЯЩ ЗА УСЛУГИТЕ НА ДОМЕЙНА IICT.BAS.BG 5

3. РАЗВИТИЕ НА ДОМЕЙНА BAS.BG И ПОДДОМЕЙНА IICT.BAS.BG 6

4. УЕБ СЪРВЪР ЗА ОСНОВНИТЕ ДОМЕЙНИ В ИИКТ 8

4. СЪРВЪР ЗА ЕЛЕКТРОННА ПОЩА MAIL.IICT.BAS.BG 13

5. FTP УСЛУГИ КЪМ IICT.BAS.BG 21

6. ОБЕЗПЕЧАВАНЕ НА КРИПТОГРАФСКИТЕ СРЕДСТВА ЧРЕЗ ГЕНЕРАТОР НА СЛУЧАЙНИ ЧИСЛА 22

ЗАКЛЮЧЕНИЕ: ПРЕМИНАВАНЕ ОТ УПРАВЛЕНИЕ НА РЕСУРСИ КЪМ УПРАВЛЕНИЕ НА УСЛУГИ В ОБЛАК С ПОВИШЕНА КИБЕРСИГУРНОСТ. 25

ИЗПОЛЗВАНА ЛИТЕРАТУРА 26

УВОД: ЦИФРОВА ТРАНСФОРМАЦИЯ И КИБЕРУСТОЙЧИВОСТ НА ИИКТ-БАН - Е-ИНФРАСТРУКТУРА И СИГУРНОСТ.

В изпълнение на Стратегията за развитие на ИИКТ-БАН до 2030 (2019 година) и в частност целта за повишаване на ефективността, ефикасността, киберустойчивостта и икономичността в управление на ИТ ресурсите на ИИКТ-БАН и преминаване от управление на ресурси, към управление на услуги през 2020 бе иницииран проект „.ЗОРА“.

Проектът се изпълнява на фази в спираловиден модел за всеки 3 години:

консолидация на инфраструктурата и повишаване на киберустойчивостта (2020);

усъвършенстване на управлението на ресурсите (2021);

преминаване към управление на услуги (2022).

В организационен план проект ЗОРА включва установяване на Функция „Главен Информационен Мениджър“ (служител/секретар по информационен мениджмънт) и „Секретар по мрежова и информационна сигурност“ (киберсигурност), заедно със служител по защита на личните данни (GDPR), системен администратор на ИИКТ-БА и системни администратори на звената (секциите) на ИИКТ-БАН.

За подготовка на служителите в горните роли по изпълнение на документираните функции се подготвиха три е-курса (отделен репорт в IT4Sec серията):

Управление на информационните ресурси и услуги / ГИМ;

Системна администрация в сложни (федерирани) организации;

Киберхигиена в сложни (федерирани) организации.

Този репорт е основно разработен от **Иван Благоев, Илиян Илиев** под ръководството на доц. Шаламанов, като инициатор на проект ЗОРА.

Документът отразява преходът към домейн **iict.bas.bg** около който се консолидира е-инфраструктурата на ИИКТ-БАН с последваща виртуализация, повишаване на киберсигурността и преминаване към управление на услуги за реализация на концепцията на „Център за споделени ИТ услуги“.

Развитието на проекта ще включи сравнение на развитието на домейна **iict.bas.bg** с домейна **acad.bg** (БИОМ) с цел извличане на добри практики и разпространението им в двата домейна, както и постигане на по-добро взаимодействие между двата домейна.

Целта е постигнатото в домейн **iict.bas.bg** да бъде разширено в домейн **bas.bg** като основа за цифрова трансформация и киберустойчивост на БАН и създаване на „знанийно езеро“ за натрупване на знания чрез изследвания и гъвкава / адаптивна система за е-обучение по разпространение на това знание в интерес на трансформация на публичната администрация и икономиката, а във взаимодействие с Института по отбрана на МО и на трансформация на сектора за сигурност.

Проект ЗОРА е подготвително усилие за иницииране на Проект за цифрова трансформация и киберустойчивост на БАН по Плана за възстановяване и устойчивост и в съответствие с препоръките на Консултативния съвет по ефективност, ефикасност и киберустойчивост в управление на ИТ ресурсите на БАН при Председателя на БАН (председател проф. Аврам Ескенази).

Проект ЗОРА се изпълнява в рамките на План за ефективно, ефикасно, икономично киберустойчиво управление на информационните ресурси и експлоатация на данните в ИИКТ, разработен от Главния информационен мениджър с участието на служителя за

мрежова и информационна сигурност, и служителя по защита на личните данни с финансиране от „собствени средства“ на института. Целта е при оптимизация на управлението на информационните ресурси и експлоатация на данните да се стигне то Център за споделени ИТ услуги (ЦСИТУ) за всички секции и звена на ИИКТ-БАН (който да прерасне в ЦСИТУ за всички звена на БАН, а напред във времето и на всички академични звена в България). За поддържане на този трансформационен процес се подготвя проект за консолидиране на експертиза и инфраструктура в „Лаборатория по цифрова трансформация и киберустойчивост“ в ИИКТ-БАН (Зала 2).

По-долу в този доклад са описани постиженията в изграждане на основната е-Инфраструктура и сигурност по Плана за ефективно, ефикасно, икономично киберустойчиво управление на информационните ресурси и експлоатация на данните в ИИКТ през 2021 година с ориентация към целите за 2022 година. Въпросите по е-обучение за цифрови компетентности и за развитие на уеб-услугата, услугата за телеконференции са в отделни доклади.

Развитието на пакет от услуги „Цифрово работно място“ цели въвеждане на нов модел за работа, при който дистанционно или присъствено чрез виртуализирана (частен облак) и сигурна е-Инфраструктура сътрудниците на института (на постоянна работа и по проекти) ще могат да ползват по оптимален начин всички ресурси при съответните права на достъп (профили), както и да се предоставя „Цифрово работно място“ като услуга на външни организации, отделни потребители в сферата на компетентност на института. Това е особено важно за развитие на старт-ъп инициативи с необходимост до специализирана е-Инфраструктура, развивана в ИИКТ-БАН.

1. СВЪРЗАНОСТ НА УСЛУГИТЕ КЪМ ДОМЕЙНА IICT.BAS.BG

Свързаността на всички услуги се осигурява чрез един Firewall рутер пред сървъра на домейна iict.bas.bg. Рутерът е MikroTik CCR1009-7G-1C-1S+, който е с висока производителност и е актуализиран с всички съвременни функции предоставяни от производителя към момента. Отговаря за свързаността на всички услуги хоствани от сървъра iict.bas.bg по двата комуникационни протокола IPv4 и IPv6. Изпълнява функциите на Firewall, като блокира достъпа до определени портове към услуги, които трябва да са недостъпни от глобалната комуникационна мрежа Интернет и по двата протокола IPv4 и IPv6. Разпределянето на трафика по двата протокола към сървъра се извършва по два физически интерфейса. Целта е двата протокола да се отделят, за да се постигне по-висока производителност и по-добро администриране на различни правила за комуникация и сигурност. Връзката, която се осигурява и обработва от рутера и сървъра в реално време в Интернет е високо скоростна от 1 Gbps в двете посоки (Upload/Download).

2. СЪРВЪР ОТГОВАРЯЩ ЗА УСЛУГИТЕ НА ДОМЕЙНА IICT.BAS.BG

Всички услуги към домейна iict.bas.bg са виртуализирани и работят върху сървърен хардуер SuperMicro модел SYS-5019C-WR, който е еднопроцесорна машина с процесор Intel(R) Xeon(R) E-2236 CPU @ 3.40GHz, 32 GB RAM и два твърди диска с капацитет 4 TB работещи в RAID1. Хоста за виртуализация и виртуалната машина работят чрез ОС с отворен код Linux, както и всички услуги към домейна iict.bas.bg са върху Linux и са с

отворен код. Създадени са технически средства за автоматизирано архивиране на виртуалната машина един път седмично и съхраняването на бекъп копия на ротационен принцип до два месеца назад в заделено за тези цели хранилище.

Развитието предвижда поддържане на втори физически сървер, както и възможност за създаване на виртуално машини върху суперкомпютъра Авитохол за нови експериментални услуги (напр. Мудъл сървер).

Сървърът е защитен с UPS и при поставянето на втори физически сървер в „огледален режим“ ще може да се осигури непрекъсваемост на поддръжката на „частния облак“ за услуги в iict.bas.bg.

3. РАЗВИТИЕ НА ДОМЕЙНА BAS.BG И ПОДДОМЕЙНА IICT.BAS.BG

В хода на еволюцията на дадена организация, независимо от началното ѝ икономическо и техническо ниво на развитие, но поемаща в посока към сложна федерация, като неизменна част от този процес в исторически план, винаги се наблюдава количествено натрупване на системи, работещи както едни с други, така и предоставящи услуги на членовете на организацията. Чисто естествено този процес изисква описание на ресурсите, по начин, по който те да бъдат разпознаваеми от една страна, както за машини и услуги, така и за хората, а от друга – да дават непосредствена количествена оценка. Ако се абстрахираме, че машините така или иначе могат да пренасят информация между източник и местоназначение (конкретно едно „Unicast“, някое „Anycast“, няколко „Multicast“ или широко „Broadcast“), с използване на съответните механизми на адресация според конкретния протокол, без допълнително знание от особено значение, то запомнянето на всичко това от страна на човек в даден момент би станало немислимо. Едно от решенията е, да се използва тетрадка, в която се описват правите релации име на ресурс – адрес, като се започне от първа страница и същевременно от последната страница, при завъртане на тетрадката на 180 градуса, започва описването на обратните релации адрес – име. При срещане на правите и обратните реалации, обикновено след средата на тетрадката, тъй като чисто статистически правите записи и промените в тях са повече, тогава се издава продължение. За надлежно водене на тетрадковия механизъм трябва да бъдат назначени отговорник на физическите ресурси (химикалки, тетрадки, перфоратор, класьори, кашони за съхранение, тиксо), главен редактор, писар и удостоверителен орган, който да подписва валидността на внесените редакции – добавяне, промяна, изтриване на ред. За свеждане на данните от тетрадката до знанието на членовете на огранизацията и имплементирането на това знание от тяхна страна в конкретиката на дадена система, е необходимо да се тиражират записите в други тетрадки, които бихме могли да ги наречем подчинени, а първоизточникът на знанието – главна тетрадка. Броят на подчинените тетрадки по звена зависи от потребността на организацията относно това, знанието за системите да стига до членовете винаги актуално. За водене на преписите в подчиненията тетрадки трябва да бъдат назначени отново отговорник на физическите ресурси, писар и главен редактор, който да следи за нов тираж на записи от главната тетрадка, съответно на главният редактор на главната тетрадка му се вменява задача да уведомява подчинените за нов тираж и да тиражира промените към подчинените тетрадки с валиден подпис на удостоверителния орган към момента на внесената редакция. При последващо разширение на организацията с обособени големи звена в клонова мрежа, същите могат да оперират в собствени мрежови сегменти и пространства за имена. Тогава възниква необходимостта от пренасяне на политиките и практиките от щаба на организацията към клоновата мрежа и респективно

клонът трябва да ръководи самостоятелно механизмите на тетрадковата си система с главни, подчинени тетрадки, тиражи, перфоратори, кашони и всичко около процеса. Това може да се осъществи, когато в главната тетрадка се внесат специални редове, описващи тетрадките на клоновата мрежа, наречени отговорни тетрадки и между удостоверителните органи на щаба и клоновете се изгради верига на доверие, така че за осъществените редакции в клона да се гледа на тях с доверие в щаба. Всичко дотук би работило гладко, ако светът не беше безкомпромисен към всяка политическа доктрина, налагащ ѝ изграждане на отношения между различни лагери. Организациите започват да общуват помежду си и се появяват първите проблеми: 1. в тетрадките трябва да се поддържат различни релации за видимостта на един и същ ресурс при използването му във или отвън организацията, 2. всяка организация трябва да знае, кой/кое тиражира записите за съответната друга организация, с която поддържа отношения, 3. трябва да се вярва на тиражите, 4. в съвременния свят дори отделни членове използват мрежова връзка през пробити малки организации за достъп до важни ресурси на организацията си, което налага 4.1. тетрадките трябва да осигуряват високо ниво на автентичност на информацията, 4.2. тиражите да се разпространяват своевременно през ненадеждния доставчик, на който не му влиза в интересите да осъществява добра услуга с бързо разпространение, 5. появяват се крайни клиенти на организацията със същите проблеми от т.4. Така тетрадките са заменени от автоматизирана клиент-сървър система DNS, организирана йерархично с коренови (ROOT) сървъри, на които се вярва безпрекословно; Top Level Domain зони, подчинени на ROOT, които поддържат записите за отговорните сървъри за всяка оргранизация; регистрари, които запазват уникални имена за дадена организация, публикуват отговорните му сървъри за имена в горната зона и хешират публичните ключове, кореспондиращи на частните, с които е извършено подписването на записите от тиражите за съответната зона, обличащи изброеното в търговска дейност. При обратните релации, логиката е идентична, като вместо TLD има ARPA зони, подчинени на кореновите ROOT сървъри. Въведената в света DNS система от 1983 г. решава постепенно всички проблеми до наши дни с изключение на 4.2, като за решаването на този проблем се използват други похвати, напр. тунелни механизми между къщите на членовете и организацията.

Във връзка с развитието на услугите в домейн зоните BAS.BG, IICT.BAS.BG и прилежащите им мрежови ресурси, е необходимо:

1. Отговорните сървъри на BAS.BG (ns.bas.bg, ns1.bas.bg, ns2.bas.bg) да поддържат DNNSEC с актуалните алгоритми към момента по отношение на степента на сигурност и да са под контрола на организацията.

2. Отговорните сървъри сървъри на IICT.BAS.BG (ns1.bas.bg, ns2.bas.bg) да се трансформират в собствени за IICT.BAS.BG (ns1.iict.bas.bg, ns2.iict.bas.bg) и да са под контрола на ИИКТ. Да поддържат DNNSEC с актуалните алгоритми към момента по отношение на степента на сигурност.

3. Да се заделят първоначално поне два мрежови сегмента /24 IPv4 и /64 IPv6 от пространството на БАН, които да се маршрутизират статично през рутера на ИИКТ, а след време още 2 такива от други подмрежи за бъдещи цели по огледалност и резервираност на услугите в случай на отпадане на 1 точка.

4. PTR записите от съответните ARPA зони за мрежовите сегменти от т.3 да са под контрола на бъдещите NS сървъри на ИИКТ ns1.iict.bas.bg, ns2.iict.bas.bg. Да поддържат DNNSEC с актуалните алгоритми към момента по отношение на степента на сигурност.

4. УЕБ СЪРВЪР ЗА ОСНОВНИТЕ ДОМЕЙНИ В ИИКТ

Уеб сървър осигуряващ всички Уеб услуги на следните домейни:

iict.bas.bg – е основен домейн, корен на всички под-услуги, които трябва да са достъпни и разпознаваеми в глобалното Интернет пространство. Като към този домейн е прикачен Уеб порталът на института и отговаря за работата на електронната поща.

mail.iict.bas.bg – този под-домейн отговаря за техническото обслужване на електронната поща. Всички машини от страна на ИИКТ и трети страни разчитат на този специализиран запис, за да открият услугата за електронна поща на Института.

mta-sts.iict.bas.bg – подпомагащ домейн, насочващ към технология създадена от лабораториите по кибер сигурност на Google, за защита на пощенските услуги от едни от най-опасните хакерски атаки: man-in-the-middle

webmail.iict.bas.bg – Уеб клиент за работа с електронната поща на домейна iict.bas.bg. На този домейн потребителите намират напълно функционална Уеб поща, която е винаги достъпна през Уеб браузър.

ailt.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници. Ползва се и за индивидуален сайт на секцията, представящ нейната научна дейност и постижения.

cit.iict.bas.bg – електронен вариант на списанието „Cybernetics and Information Technologies“ към ИИКТ. Достъпва се през Уеб браузъри и е оптимизирано за индексиране от търсещи машини в Интернет. Съдържа електронен архив на изданията си от 2001 г. до днес.

cps.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници. Ползва се и за индивидуален сайт на секцията, представящ нейната научна дейност и постижения.

css.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници. Ползва се и за индивидуален сайт на секцията, представящ нейната научна дейност и постижения.

rius.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници. Ползва се и за индивидуален сайт на секцията, представящ нейната научна дейност и постижения.

ipdss.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници. Ползва се и за индивидуален сайт на секцията, представящ нейната научна дейност и постижения.

is.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници. Ползва се и за индивидуален сайт на секцията, представящ нейната научна дейност и постижения.

it4sec.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници.

mo.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници.

pa.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници.

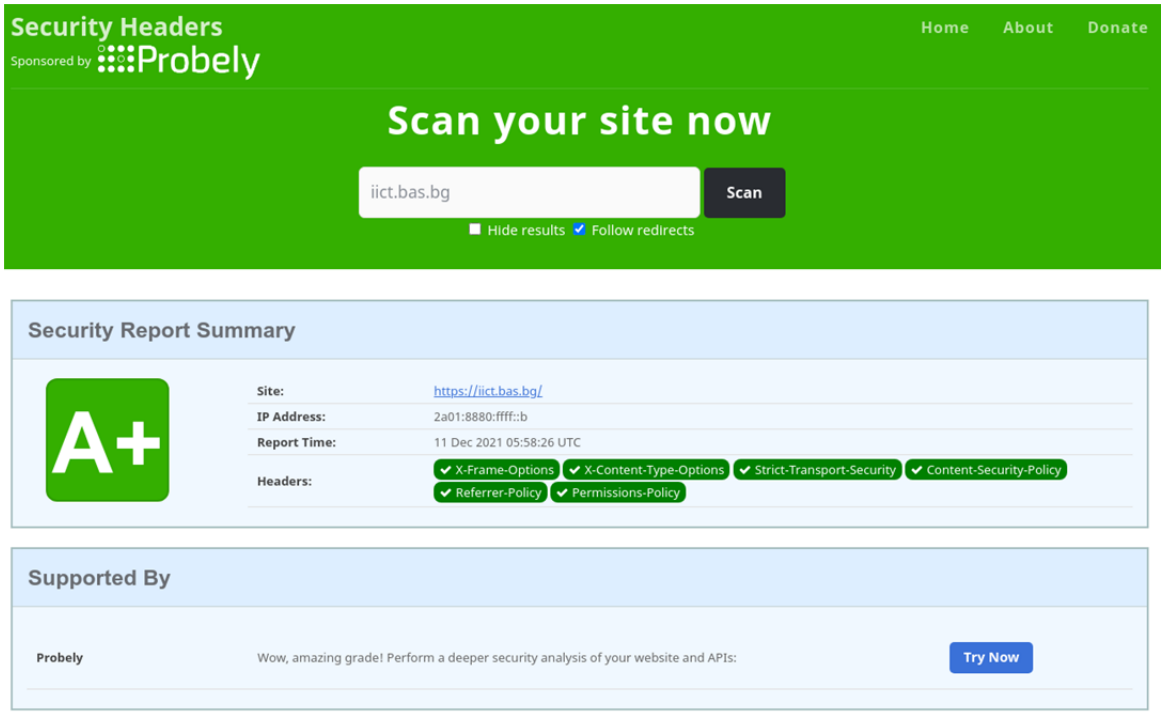
pecr.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници.

sca.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници.

sc.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници.

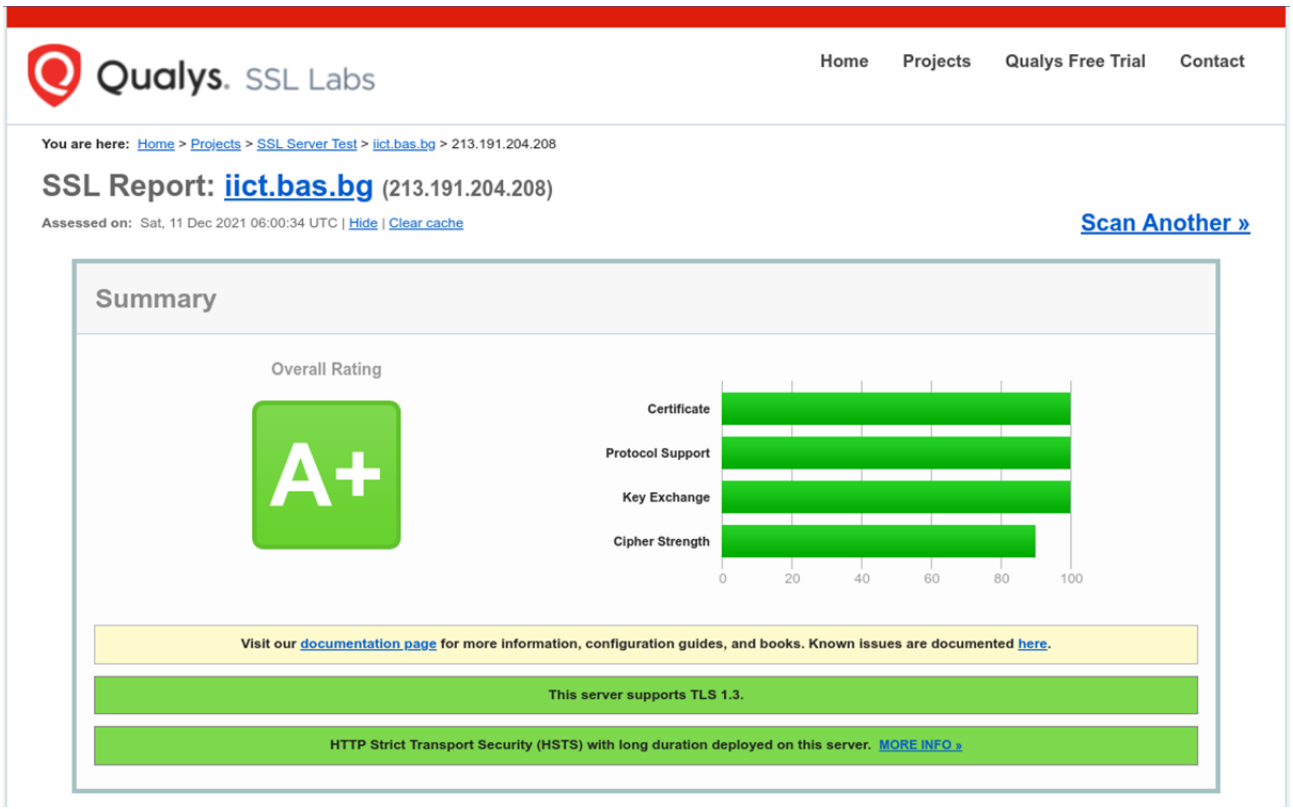
sdp.iict.bas.bg – Облачно пространство за споделяне на съдържание от секциите на ИИКТ. Разпознава се за комуникация чрез FTP и Уеб браузър. Помага на потребителите да споделят научно съдържание с различни Интернет източници.

Хостинг сървърът е осигурен от високо производителен Уеб сървър NGINX, което позволява да се обработват голям брой едновременни заявки от клиентски-потребителски сесии с относително малко оперативна памет на основата комуникационния принцип т.нар. „кръг от събития“ за разлика от традиционните нишкови приложения на уеб услуги при приложните сървъри. Нивото на кибер защита на уеб услугите е най-високото към настоящия момент. В потвърждение са направени редица тестове от сканиращи системи на външни организации, които са във връзка и в съгласие с кибер лабораториите (FIPS, NIST, Common criteria) и резултатите са приложени в този отчет. Уеб сървърът е конфигуриран да не допуска известните към момента видове кибер атаки[13,14,15] срещу Уеб услуги[6,7,8,9]. Като доказателство се прилага тест на независима организация, за оценка на кибер защитата при Уеб услугите Probey - Web application and API vulnerability scanner, който оценява Уеб услугите на iict.bas.bg с най-високото ниво на защита (A+), фиг. 1:

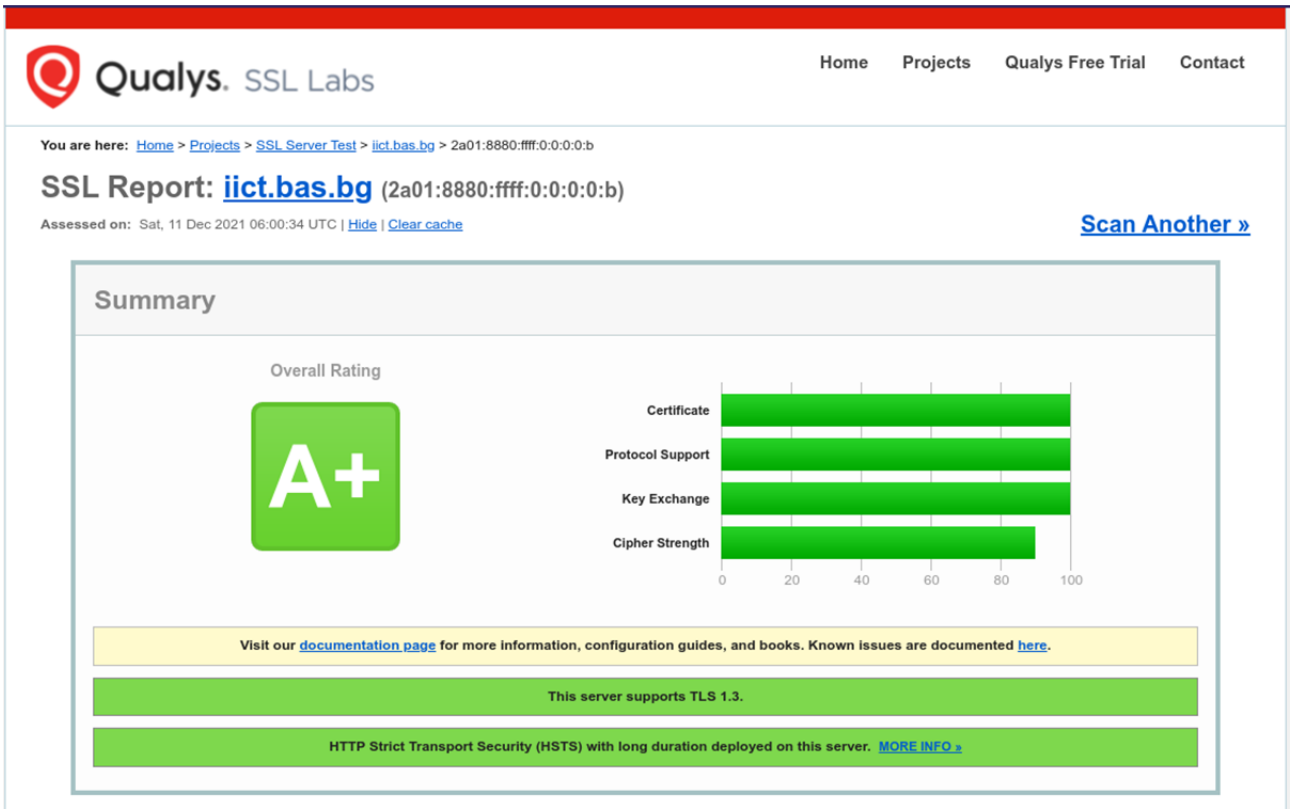


Фиг. 1. Оценка за кибер защита на Уеб сървър

Криптографската защита на Уеб услугите е в съгласие с всички съвременни изисквания за кибер и криптографска сигурност[10] при този вид услуги, според утвърдените стандарти FIPS, NIST и Common criteria. Като основен протокол за тунелна криптографска свързаност между клиент-сървър е TLSv1.3, който е последната версия за момента. Поради съвместимост с по-стари устройства е допуснат и протокол TLSv1.2, но с ревизиран списък с криптографски алгоритми, които са също към момента одобрени според съвременните утвърдените стандарти (FIPS, NIST [10], Common criteria [11]). В допълнение, се прилага тест на SSL Labs, който тества качеството на TLS протокола за тунелна и криптографска свързаност между клиент и сървър и на двата комуникационни протокола TCP/IPv4 и TCP6/IPv6, като оценката е най-високата възможна (A+), Фиг.2 и Фиг.3:



Фиг. 2 Оценка за криптографска свързаност по IPv4

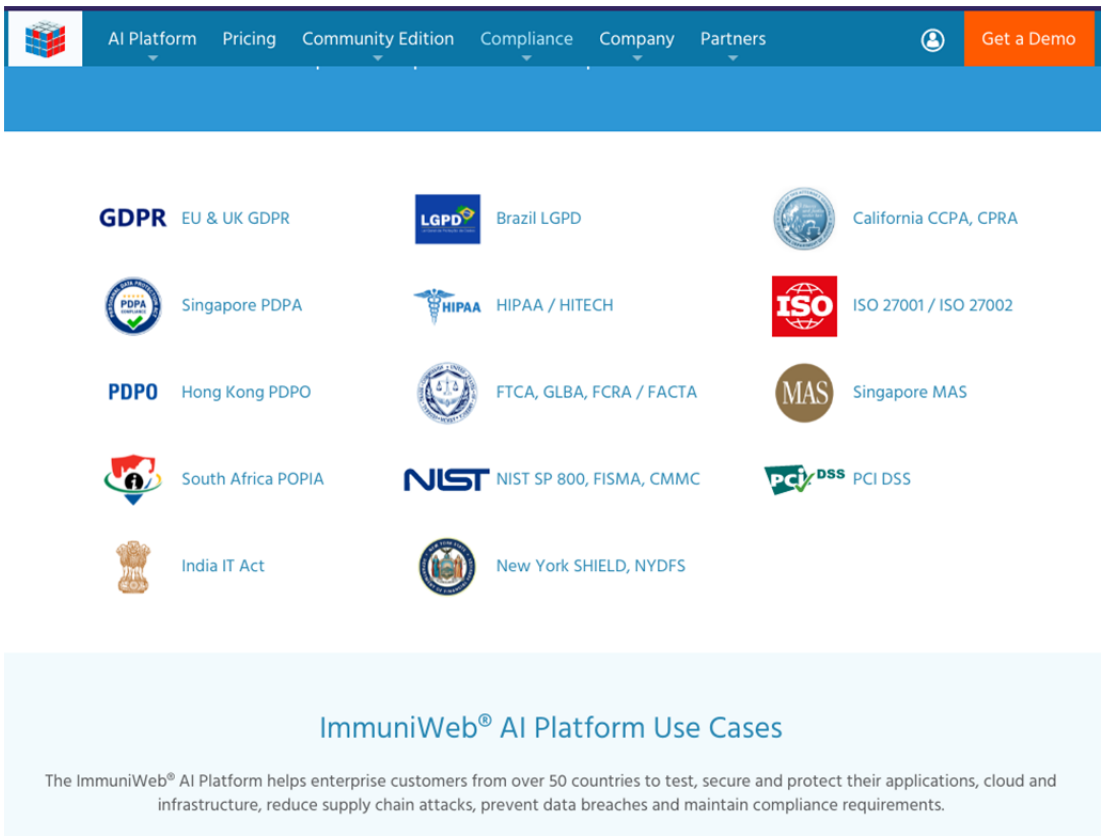


Фиг. 3 Оценка за криптографска свързаност по IPv6

В допълнение е приложен тест и от друга система за проверка качеството на кибер защитата на immuniweb, които извършват своите тест и анализ по следните критерии:

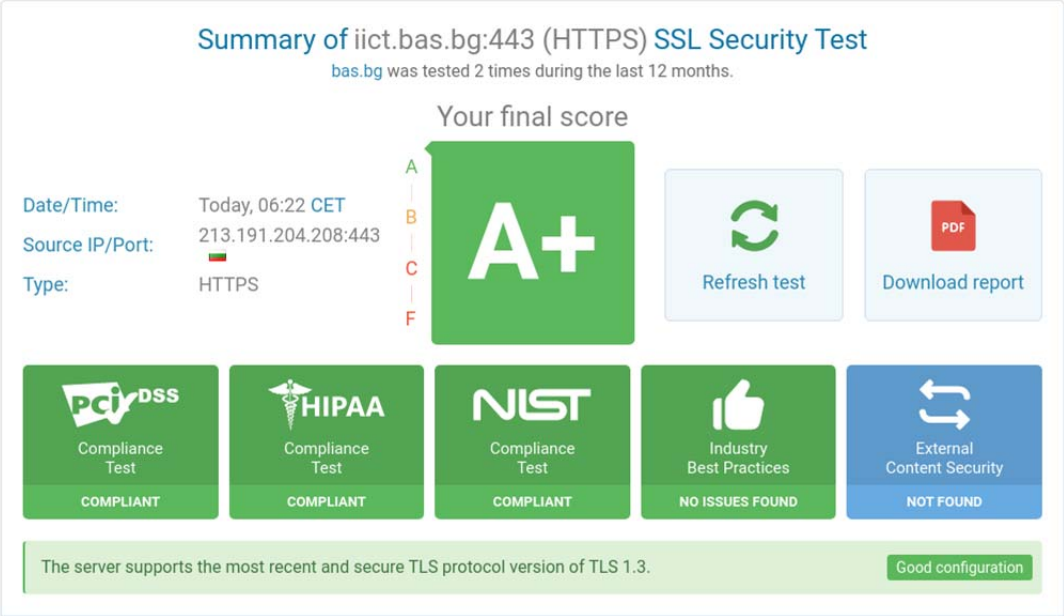
1. Testing SSL/TLS for PCI DSS compliance
2. Testing SSL/TLS for HIPAA guidance
3. Testing SSL/TLS for NIST guidelines
4. Testing SSL/TLS for industry best practices

В тези четири критерия са събрани съвременните изисквания според следните организации и стандарти (фиг.4):



Фиг.4 ImmuniWeb Cybersecurity Compliance List

Резултатът за нивото на кибер защита на всички уеб услуги в домейна iict.bas.bg отново получават най-високата степен на оценка (A+), като резултатът е направен на базата на над 200 теста върху кибер сигурността на Уеб услугите по критерии на изброените по-горе организации и стандарти:

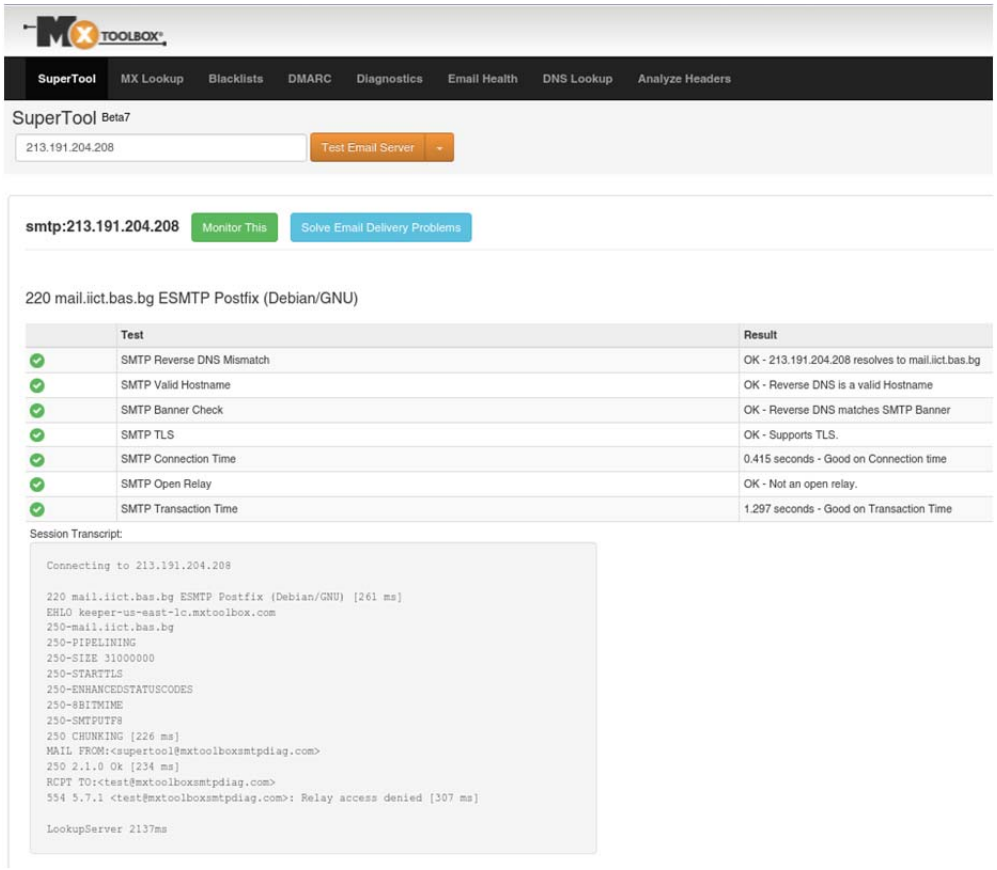


Фиг.5 ImmuniWeb оценка за криптографска свързаност

5. СЪРВЪР ЗА ЕЛЕКТРОННА ПОЩА MAIL.IICT.BAS.BG

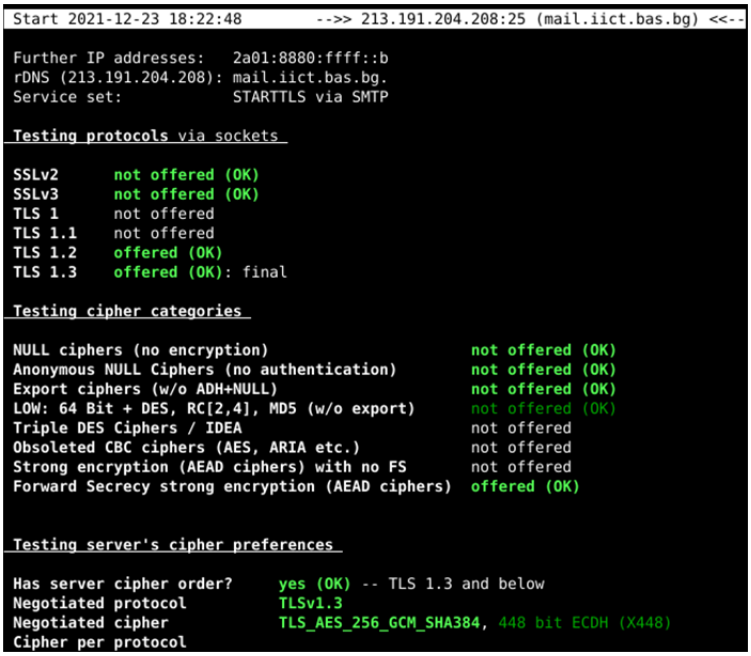
Сървърът за електронна поща към настоящия момент обслужва 256 потребителски акаунта. Достъпа до неговите услуги може да се извършва през компютърен клиент за електронна поща, преносими устройства (мобилни телефони, таблети и др.), потребителски Интернет браузър. Пощенските протоколи са достъпни само чрез криптографска защита от типа TLSv1.3 и по съвместимост TLSv1.2. При TLSv1.2 списъкът от поддържаните алгоритми е ревизиран само до одобрения според съвременните стандарти за криптографска и кибер защита на FIPS, Common criteria, NIST. Защитата се удостоверява с SSL/TLS сертификата за сървърна идентификация, издаден от Sectigio, който е сертифициран Удостоверяващ орган и е защитен с удостоверителната верига на доставчика. Криптографският алгоритъм, който го подсигурява е Secp384r1 и е одобрен от лабораториите на FIPS, NIST, Common criteria за криптографска и кибер защита[10,11].

Комуникационните протоколи, по които е достъпна пощенската услуга са IPv4 и IPv6, които се маршрутизират и защитават от Firewall – рутер MikroTik CCR1009-7G-1C-1S+ специално инсталиран и конфигуриран за целта.



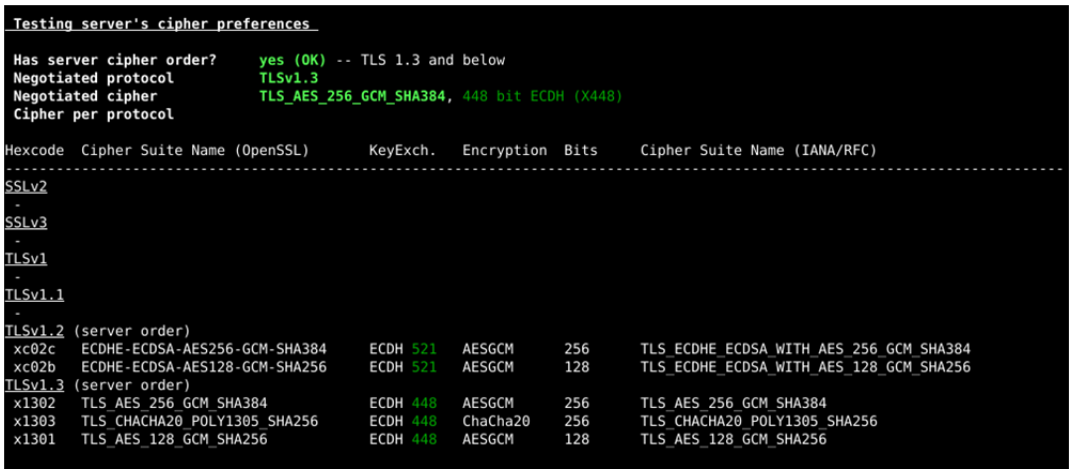
Фиг.6 Проверка качеството на свързаност и работоспособност на услугата за електронна поща: mail.iict.bas.bg

Пощенската услуга има интегрирана антивирусна защита, автоматично проверяваща входящ/изходящ пощенски трафик. Интегрирана е защита и за непоискана поща, като се проверява рейтинга на входящите податели на поща към международни черни списъци и ранг за компрометирани пощенски сървъри. Извършва се и анализ на получаваните електронни писма според алгоритми за откриване на непоискани съобщения чрез SpamAssasin, в резултат на което, получаването на непоискани и компрометирани пощенски съобщения към потребителите е сведен под 1%. Криптографската защита за предаване на електронната поща между сървъри и от и към потребители е в съответствие с утвърдените стандарти за това според FIPS, NIST, Common criteria [10,11]. Стари и уязвими криптографски протоколи и алгоритми не се поддържат, както са покрити и уязвимостити, като уязвими cryptography paddings и компресия по протоколите за комуникация [16]. Виж фиг.7:

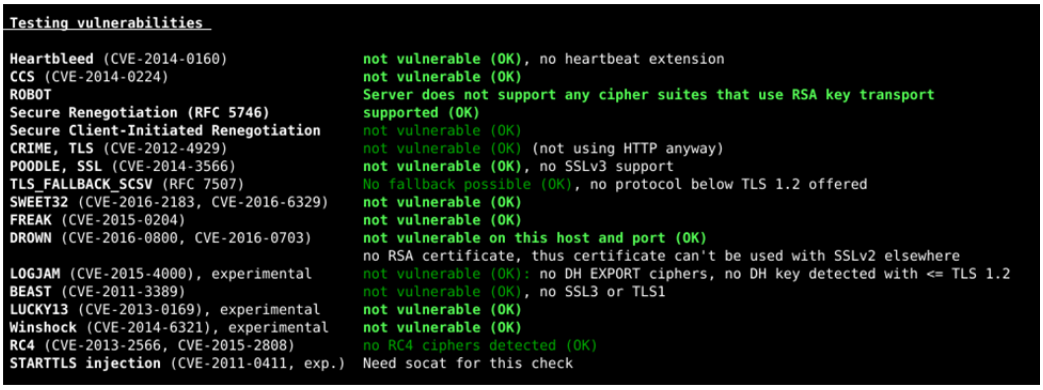


Фиг.7 Поддържани протоколи и проверка за уязвимости

Поддържаните протоколи за криптографска тунелна свързаност, осигуряващи услугата за електронна поща се обслужват само от TLSv1.3 и TLSv1.2 и сертификати за идентификация с асиметричен алгоритъм за криптиране, разчитащ на непредсказуемостта на резултата от алгебрични операции в крайно поле на дадената елиптична крива [12]. Което е видно от изходните данни на Фиг.8. Алгоритъм за асиметрична криптография RSA също е премахнат от списъка с използваните алгоритми, поради откритите в последно време уязвимости [3], виж Фиг.9.

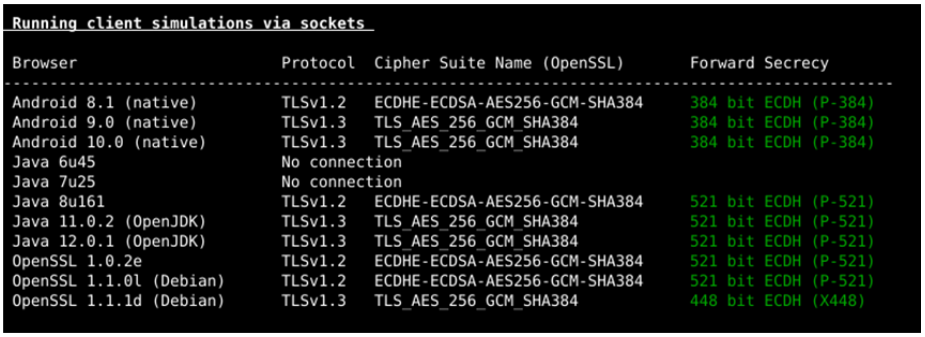


Фиг.8 Поддържани протоколи за криптогравска тунелна свързаност и алгоритми от симетричен и асиметричен тип в тях



Фиг.9 Отсъствие на известните уязвимости в криптографските протоколи, както и алгоритъма RSA

Нивото на зрялост на протоколите за криптографска кибер защита за тази услуга достига степента на актуалност на съвременните стандарти за това, поради което, някои технологии и операционни системи вече не са в списъка за работа с тази услуга (като стари версии на ОС Windows, Android, стари комуникационни интерфейси за Java и други). Настоящото ниво на зрялост се представя чрез съкратен списък за съвместимост на криптографските протоколи с някои системи, виж фиг.10:



Фиг.10 Съкратен списък на минимална версия на системи за връзка с предоставяните услуги за електронна поща

По отношение на защита на пощенската услуга от известните видове атаки (получаване на непоискана поща, идентифициране пред трети страни и други) са приложени всички известни съвременни технологии като:

- проверка за валидност на сървъри;
- криптографска идентификация;
- проверки по черни списъци за репутация на пощенски услуги;

Интегрирана е DomainKeys Identified Mail (DKIM) защита за идентификацията насъобщенията чрез подписване на значимите за пощенската комуникация хедъри и последващото им валидиране от отсрещната страна с криптография на основата на частен-публичен ключ. Добавена е защита по рейтинг на трети страни, комуникиращи с mail.iict.bas.bg. Внедрена е автоматизирана антивирусна и анти-спам защита за сканиране на целия входящ/изходящ пощенски трафик. Приложени са технологии за предотвратяване на man in the middle атаки, една от които е най-скоро създадената технология SMTP MTA Strict Transport Security (MTA-STS) от лаборатории на Google за кибер защита. Като доказателство за работоспособността на тези технологии се прилагат доклади от тестовете на различни Интернет организации, виж Фиг.11 и следния отчет на DKIMValidator.com:

Email Validation Results

Address: l4d7mnthvocufq@dkimvalidator.com

Original Message:

Received: from mail.iict.bas.bg (mail.iict.bas.bg [213.191.204.208])
by relay-8.us-west-2.relay-prod (Postfix) with ESMTPS id 5294E25875
for <l4D7mnTHVOcUfq@dkimvalidator.com>; Thu, 23 Dec 2021 17:08:32 +0000 (UTC)
Received: from mail.iict.bas.bg (localhost [127.0.0.1])
by mail.iict.bas.bg (Postfix) with ESMTP id A8DD1960412
for <l4D7mnTHVOcUfq@dkimvalidator.com>; Thu, 23 Dec 2021 19:08:30 +0200 (EET)
Received: from [192.168.2.17] (mail.omegasystems.eu [212.5.154.14])
(using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
key-exchange ECDHE (P-521) server-signature ECDSA (P-384) server-digest SHA384)
(Client did not present a certificate)
by mail.iict.bas.bg (Postfix) with ESMTPSA id 889579601F4
for <l4D7mnTHVOcUfq@dkimvalidator.com>; Thu, 23 Dec 2021 19:08:30 +0200 (EET)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=iict.bas.bg; s=mail;
t=1640279310; bh=RCCtoHlQBbPk7fHkJqwrt8hjFOTZHZjRT0OnPe/e55M=;
h=To:From:Subject:Date:From:Sender:To:CC:Subject:Date;
b=GMwh8D7K8Y/Un3aLa5n1y8PMROxPqQrReRp8eQOdNbmf5e5eh+Qrsj85h7LsZYtae
slp6ecI4dhKpI2TPKx4ywY1ry18SxSMuO3/RlkPZ+ij7U+ZVaier6KyagirCKwaEx3
zlNZvvt/79T/415hx+a7mwU1AvzNgMwYtG5B/o+IOydIx3IDQL3odqLADGreSIUHM0
qtna2dVOx0U6FXv4FrgK0n5WPrrNpq8TJmtRjs0SeUzFXrz/wCvbRbQqbaXv5hmjM7
q3qlxWILKjKCBXAu+9Z0VbBhA3CzZ+VKAQ8UorE4Wv8WYk8Xmn/lZ8plyiuTEpSC8Q
DBMyWg28bFluA==
To: l4D7mnTHVOcUfq@dkimvalidator.com
From: Postmaster IICT <postmaster@iict.bas.bg>
Subject: =?UTF-8?B?0YLQtdGB0YI=?=
Message-ID: <f53a24d9-9101-93d2-28ad-b964c9727a74@iict.bas.bg>
Date: Thu, 23 Dec 2021 19:08:30 +0200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Thunderbird/78.14.0
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit
Content-Language: bg
X-Virus-Scanned: ClamAV using ClamSMTP

тест

--
Best wishes,
Ivan Blagoev

e-mail: postmaster@iict.bas.bg
website: https://iict.bas.bg

DKIM Information (DKIM Signature):

Message contains this DKIM Signature:

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=iict.bas.bg; s=mail;

t=1640279310; bh=RCCtoHlQBbPk7fHkJqwrt8hjFOTZHZjRT0OnPe/e55M=;

h=To:From:Subject:Date:From:Sender:To:CC:Subject:Date;

b=GMwh8D7K8Y/Un3aLa5n1y8PMROxPqQrReRp8eQOdNbmf5e5eh+Qrsj
85h7LsZYtae

slp6ecI4dhKpI2TPKx4ywY1ry18SxSMuO3/RlkPZ+ij7U+ZVaier6KyagirCKwaEx3

zlNZvvt/79T/415hx+a7mwU1AvzNgMwYtG5B/o+lOydIx3IDQL3odqLADGreSIUHM0

qtna2dVOx0U6FXv4FrgK0n5WPrrNpq8TJmtRjs0SeUzFXrz/wCvbRbQqbaXv5hmjM7

q3qlxWILKjKCBXAu+9Z0VbBhA3CzZ+VKAQ8UorE4Wv8WYk8Xmn/lZ8plyiuTEpSC8Q
DBMyWg28bFluA==

Signature Information:

v= Version: 1

a= Algorithm: rsa-sha256

c= Method: relaxed/simple

d= Domain: iict.bas.bg

s= Selector: mail

q= Protocol:

bh= RCCtoHlQBbPk7fHkJqwrt8hjFOTZHZjRT0OnPe/e55M=

h= Signed Headers: To:From:Subject:Date:From:Sender:To:CC:Subject:Date

b= Data:
GMwh8D7K8Y/Un3aLa5n1y8PMROxPqQrReRp8eQOdNbmf5e5eh+Qrsj85h7LsZYtae

slp6ecI4dhKpI2TPKx4ywY1ry18SxSMuO3/RlkPZ+ij7U+ZVaier6KyagirCKwaEx3

zlNZvvt/79T/415hx+a7mwU1AvzNgMwYtG5B/o+lOydIx3IDQL3odqLADGreSIUHM0

qtna2dVOx0U6FXv4FrgK0n5WPrrNpq8TJmtRjs0SeUzFXrz/wCvbRbQqbaXv5hmjM7

q3qlxWILKjKCBXAu+9Z0VbBhA3CzZ+VKAQ8UorE4Wv8WYk8Xmn/lZ8plyiuTEpSC8Q

DBMyWg28bFluA==

Public Key DNS Lookup

Building DNS Query for mail._domainkey.iict.bas.bg

Retrieved this publickey from DNS:
v=DKIM1;h=sha256;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApU/UAxr
U0lmrmqYAK4Im0TMVHm8a+LQaroe6hmDgMvfdmUEKsz9YnmFJ+2WsS5SxlAxh8w4zWH24N9
H04gkaceZ2UN/jMoY1/JBXGJ00JGq2s0I2fY4VaZg7CRFD3K6vDBrgxInwhzFKm7GFUVnFT4U/05
NcudSG/C/MAjj9uKkZ7dsQ0zXE9WgoAWO9NmYechC/G6ewN91Vq35tOavwt5zLhJGW/a3vzz5x
2GaRL7xuAMOeqkCDuOGLCFW9glSOYoEa+pzCfbS6g1/FJPhYmEy1XlpZNR60U9wqLMk92fiS
MKzJIc8j5aTlS4ng6SVTyBcdRi06u4dPV5hm8FG1UQIDAQAB

Validating Signature

result = pass

Details:

SPF Information:

Using this information that I obtained from the headers

Helo Address = mail.iict.bas.bg

From Address = postmaster@iict.bas.bg

From IP = 213.191.204.208

SPF Record Lookup

Looking up TXT SPF record for iict.bas.bg

Found the following namesevers for iict.bas.bg: ns1.bas.bg ns2.bas.bg

Retrieved this SPF Record: zone updated 20210630 (TTL = 600)

using authoritative server (ns1.bas.bg) directly for SPF Check

Result: pass (Mechanism 'mx' matched)

Result code: pass

Local Explanation: iict.bas.bg: 213.191.204.208 is authorized to use 'postmaster@iict.bas.bg' in 'mfrom' identity (mechanism 'mx' matched)

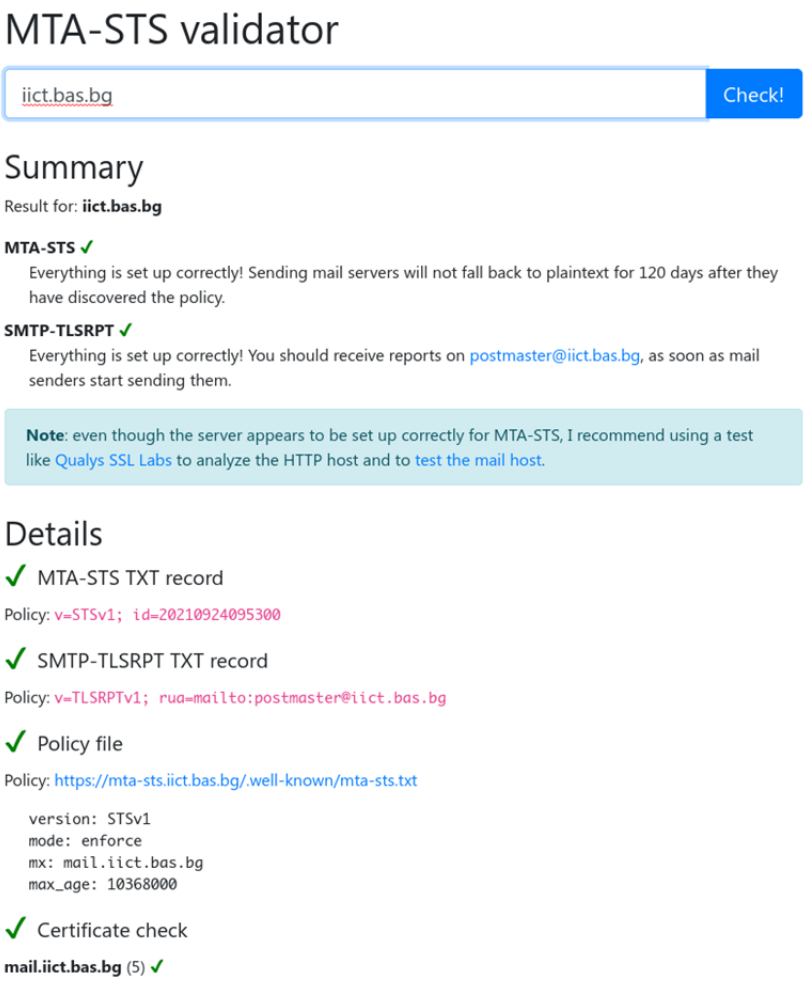
spf_header = Received-SPF: pass (iict.bas.bg: 213.191.204.208 is authorized to use 'postmaster@iict.bas.bg' in 'mfrom' identity (mechanism 'mx' matched)) receiver=ip-172-31-60-105.ec2.internal; identity=mailfrom; envelope-from="postmaster@iict.bas.bg"; helo=mail.iict.bas.bg; client-ip=213.191.204.208

SpamAssassin Score: 0.201

Message is NOT marked as spam

Points breakdown:

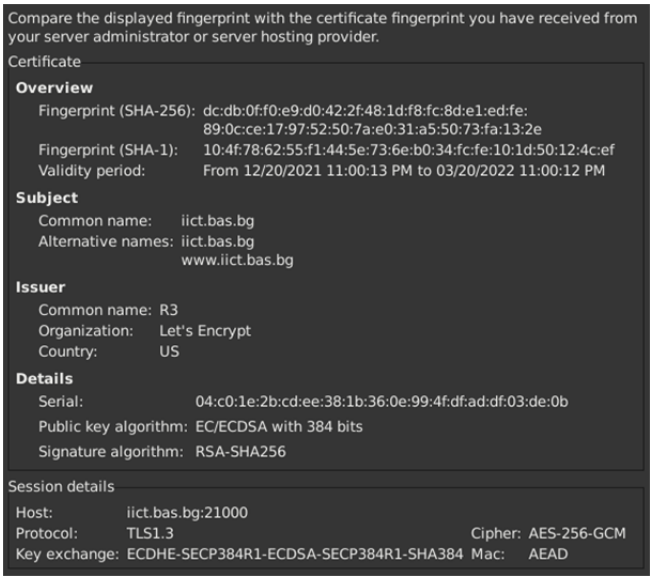
0.0 SPF_HELO_NONE	SPF: HELO does not publish an SPF Record
0.1 DKIM_SIGNED	Message has a DKIM or DK signature, not necessarily valid
0.1 DKIM_INVALID	DKIM or DK signature exists, but is not valid



Фиг.11 Резултат от анализ на MTA-STS технологията от Google Labs

6. FTP УСЛУГИ КЪМ IICT.BAS.BG

Изградено е FTP пространство за актуализиране съдържанието на Уеб портал https://iict.bas.bg/, две научни издания (https://iict.bas.bg/cit/ и https://iict.bas.bg/pecr/) и споделено пространство за секциите на ИИКТ. Услугата е защитена чрез сертификати за идентификация с асиметричен алгоритъм за криптиране, разчитащ на непредсказуемостта на резултата от алгебрични операции в крайно поле на дадената елиптична крива. Протоколите за тунелна криптографска свързаност за TLSv1.3 и TLSv1.2 с ревизиран списък с криптографски алгоритми, които са също към момента одобрени според съвременните утвърдените стандарти, като FIPS, NIST, Common Criteria [10,11] (виж фиг.12). Достъпът от страна на клиент може да се извърши и по двата комуникационни протокола IPv4 и IPv6. Защитата на услугата е в Implicit mode, което е възможно най-доброто за установяване на свръзка клиент-сървър, понеже не се допуска части от установяване на свързването да преминават без защитата на криптографските протоколи. Изготвено е ръководство за конфигуриране на FTP клиент, което да е в помощ на системните администратори отговарящи за актуализирането на съдържанието по съответните зони на сървъра.



Фиг. 12 параметри на криптографска защита на FTP услугата

6. ОБЕЗПЕЧАВАНЕ НА КРИПТОГРАФСКИТЕ СРЕДСТВА ЧРЕЗ ГЕНЕРАТОР НА СЛУЧАЙНИ ЧИСЛА

Известно е от научни изследвания [1,5], че при Интернет услуги, като представените до тук, които се намират върху един и същ физически сървър и се използват от стотици потребители едновременно, източника на случайни числа в повечето случай е недостатъчен. Поради публичността на услугите, достъпа на множество анонимни потребители към тях, комуникацията с трети страни и наличието на множество устройства у всеки един от потребителите могат да генерират хиляди заявки към сървъра. Понеже всички те (както е представено до тук), се осигуряват от криптографска защита исе нуждаят постоянно от случайни числа. За това в операционната система върху която се хостват всички тези услуги и критпграфските техники за защитата са приложени методи за повишаване капацитета на източника на случайни числа. Методите са описвани в различни изследвания по темата[2,3], но на кратко използват вграден технология в настоящия Xeon процесор. Също така са приложени и програмни средства за събиране на ентропия на информация от различни считани за случайни събития в компютърната система. Както е приложен и метод за генериране на събития, за повишаване на ентропията подпомагащ предходните технологии.

Резултатите от анализа на протоколите за криптиране се прилагат за доказателство на достатъчно бързата и качествена ентропия необходима на системата. За осигуряването на тази ентропия са използвани средства от предлаганите, като решение в изследванията до момента [3,4]. Изборът на процесор притежава специализиран силициев генератор за обогатяване на ентропията при случайните числа, достъпен с налични инструкции от ниско ниво rdrand и rdseed [3]. Следното може да се види, след прилагането на командите представени до момента в следния ред по-долу:

lscpu

Architecture: x86_64

CPU op-mode(s): 32-bit, 64-bit

Byte Order: Little Endian

Address sizes: 39 bits physical, 48 bits virtual

CPU(s): 12

On-line CPU(s) list: 0-11

Thread(s) per core: 2

Core(s) per socket: 6

Socket(s): 1

NUMA node(s): 1

Vendor ID: GenuineIntel

CPU family: 6

Model: 158

Model name: Intel(R) Xeon(R) E-2236 CPU @ 3.40GHz

Stepping: 10

CPU MHz: 800.343

CPU max MHz: 4800.0000

CPU min MHz: 800.0000

BogoMIPS: 6816.00

Virtualization: VT-x

L1d cache: 32K

L1i cache: 32K

87L2 cache: 256K

L3 cache: 12288K

NUMA node0 CPU(s): 0-11

Flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp lm constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc cpuid aperfmperf tsc_known_freq pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c **rdrand** lahf_lm abm 3dnowprefetch cpuid_fault epb invpcid_single pti ssbd ibrs ibpb stibp tpr_shadow vnmi flexpriority ept vpid ept_ad fsgsbase tsc_adjust bmi1 hle avx2 smep bmi2 erms invpcid rtm mpx **rdseed** adx smap clflushopt intel_pt xsaveopt xsavec xgetbv1 xsaves dtherm ida arat pln pts hwp hwp_notify hwp_act_window hwp_epp md_clear flush_l1d

```
# cat /proc/cpuinfo | grep -i rdrand | echo $?

0
```

Извършени са тестове и на качеството на ентропия, чрез инструментите използвани в текущото изследване [2]. От командния shell на сървъра са приложени два утвърдени инструмента, първият проверява качеството на ентропия по FIPS с rngtest, а вторият с инструмента за анализ dieharder. Преди изпълнението на двата теста е проверено нивото на ентропия натрупано в буфера, чрез съответната команда:

```
# cat /proc/sys/kernel/random/entropy_avail

3219
```

Резултати от тест качеството на ентропия с инструмента rngtest според стандарта FIPS:

```
# rngtest -c 1000 </dev/random

rngtest 5

Copyright (c) 2004 by Henrique de Moraes Holschuh

This is free software; see the source for copying conditions.

There is NO

warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

88rngtest: starting FIPS tests...

rngtest: bits received from input: 20000032

rngtest: FIPS 140-2 successes: 1000

rngtest: FIPS 140-2 failures: 0

rngtest: FIPS 140-2(2001-10-10) Monobit: 0

rngtest: FIPS 140-2(2001-10-10) Poker: 0

rngtest: FIPS 140-2(2001-10-10) Runs: 0

rngtest: FIPS 140-2(2001-10-10) Long run: 0

rngtest: FIPS 140-2(2001-10-10) Continuous run: 0

rngtest: input channel speed: (min=643.343; avg=12710.535;

max=16509.932)Kibits/s

rngtest: FIPS tests speed: (min=47.329; avg=224.928; max=244.532)Mibits/s

rngtest: Program run time: 1621642 microseconds
```

ЗАКЛЮЧЕНИЕ: ПРЕМИНАВАНЕ ОТ УПРАВЛЕНИЕ НА РЕСУРСИ КЪМ УПРАВЛЕНИЕ НА УСЛУГИ В ОБЛАК С ПОВИШЕНА КИБЕРСИГУРНОСТ.

Консолидирането на е-Инфраструктурата около сървърно ядро на ИИКТ-БАН, вкл. използване на суперкомпютър Авитохол като мощен изчислителен ресурс и памет за големи данни поставя основите за централизирано управление на информационните ресурси и повишаване на киберсигурността. Това е стъпка и към създаване на Център за споделени ИТ услуги за ИИКТ, БАН и академичната общност. Определено е необходимо взаимодействие с БИОМ и acad.bg домейна.

Това е ядро на технологичното решение в цифровата трансформация на ИИКТ-БАН и тя ще се развива с консолидиране на активната инфраструктура, добавяне на разнообразната периферия в ИИКТ-БАН (уникални прибори в различните лаборатории) за единно управление и сигурност. Преходът към услуги по единен каталог е целта на това усилие.

В технологичен план важна следваща стъпка е създаването на частен облак на ИИКТ-БАН с виртуализация на необходимите за различни проекти ресурси в сърверното ядро / суперкомпютъра и следващо ниво на повишаване на киберсигурността.

В организационен план трансформацията включва консолидацията на групата от хора с роли по изпълнение на функциите: Главен информационен мениджър, служител по киберсигурност, служител по защита на личните данни, мениджър на данните, системен администратор.

Консолидацията на организационните мерки се поддържа от програма за обучение и сертификация на ангажираните служители.

В този контекст Проект Зора по изпълнение на Стратегия 2030 за ИИКТ и Плана за развитие на информационните ресурси, като страничен ефект има влияние върху:

1. Създаване на лаборатория по цифрова трансформация и киберустойчивост за подпомагане на изследователската работа и подкрепа на функциите ГИМ/ГМИМС/СЗЛД в ИИКТ-БАН;
2. Лабораторията е по принцип и „кибер полигон“ за експериментиране на нови ИКТ решения и такива за киберустойчивост, както и за подкрепа на обучение (практически занятия) и сертификационни схеми за кибер сигурност.

Работата по Проект Зора се поддържа от редица докторантски изследвания:

1. Преминаване от управление на ресурси към управление на услуги;
2. Развитие на цифрови компетентности в подкрепа на цифровата трансформация и киберусройчивост;
3. Виртуализация и сигурност при създаване на облачни решения за ИКТ услуги;
4. Повишаване на киберсигурността с криптографски методи и др.

Всичко това ще позволи въвеждане на оптимизирани процеси по:

1. Стратегическо планиране на информационните ресурси и услуги;
2. Управление на промяната в е-Инфраструктурата и Сигурността;
3. Управление на Каталога от ИТ услуги;
4. Управление на иновациите в е-Инфраструктурата и Сигурността;

5. Развитие на партньорството за разширяване на е-Инфраструктурата и Сигурността;
6. Бизнес планиране за е-Инфраструктурата и Сигурността;
7. Одит и повишаване на нивото на зрялост на е-Инфраструктурата и Сигурността.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Ivan Blagoev, Neglected Cybersecurity Risks in the Public Internet Hosting Service Providers, Information & Security: An International Journal, Volume 47, Issue 1, ISSN 0861-5160 (print), ISSN 1314-2119 (online), p.62-76 (2020), https://doi.org/10.11610/isij.4704, https://bpos.bg/publication/18454

[2] Ivan Blagoev, Method for Evaluating the Vulnerability of Random Number Generators for Cryptographic Protection in Information Systems, Print ISBN 978-3-030-55346-3, Online ISBN 978-3-030-55347-0, https://doi.org/10.1007/978-3-030-55347-0_33, https://bpos.bg/publication/18449

[3] Ivan Blagoev, Todor Balabanov, Iliyan Iliev, RSA Weaknesses Caused by the Specifics of Random Number Generation, ISSN 0861-5160 (print), ISSN 1314-2119 (online), vol. 50, no. 2 (2021): 171-179, https://doi.org/10.11610/isij.5028, https://bpos.bg/publication/18445

[4] Ivan Blagoev, Application of Time Series Techniques for Random Number Generator Analysis, Proceedings of XXII Int. Conference DCCN 2019, September 23-27, 2019, Moscow, Russia, pp.437-446. ISBN 978-5-209-09683-2

[5] Ivan Blagoev, Method for Evaluating the Vulnerability of Random Number Generators for Cryptographic Protection in Information Systems, HPC 2019: Advances in High Performance Computing pp 391-397, Conference from 2-nd to 6-th of September 2019, Print ISBN 978-3-030-55346-3, Online ISBN 978-3-030-55347-0, http://dx.doi.org/10.1007/978-3-030-55347-0_33

[6] Calzarossa, M.C., Massari, L.: 'Analysis of header usage patterns of HTTP request messages'. Proc. – 16th IEEE Int. Conf. on High Performance Computing and Communications, HPCC 2014, 11th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2014 and 6th Int. Symp. on Cyberspace Safety and Security, 2014, pp. 847–853

[7] Hodges, J., Jackson, C., Barth, A.: 'HTTP strict transport security'. Available at http//tools.ietf.org/html/rfc6797. 2012

[8] Yusof, I., Pathan, A.S.K.: 'Mitigating cross-site scripting attacks with a content security policy', Computer (Long Beach Calif.), 2016, 49, (3), pp. 56–63

[9] Kranch, M., Bonneau, J.: 'Upgrading HTTPS in Mid-Air: an empirical study of strict transport security and Key pinning'. [cited 2017 May 26]. Available at https://www.internetsociety.org/sites/default/files/Upgrading HTTPS in Mid-Air- An Empirical Study of Strict Transport Security and Key Pinning.pdf

[10] General Security Requirements for Equipment Using the Data Encryption Standard, PublishedApril 14, 1982, Report Number 140, NIST Pub Series Federal Inf. Process. Stds. (NIST FIPS), https://www.nist.gov/publications/general-security-requirements-equipment-using-data-encryption-standard?pub_id=917971

[11] Common Criteria for IT security evaluation, January 2017, https://www.commoncriteriaportal.org/files/epfiles/Cible_Lite_2017_02.pdf

[12] Darrel Hankerson, Alfred J. Menezes, Scott Vanstone, Guide to Elliptic Curve Cryptography (Springer Professional Computing) 2004th Edition, ISBN-13: 978-0387952734, ISBN-10: 038795273X

[13] Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws 1st Edition, ISBN-13: 978-0470170779, ISBN-10: 0470170778, October 22, 2007

[14] Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition, ISBN-13: 978-1118026472, ISBN-10: 1118026470, September 27, 2011

[15] Mike Meyers, Scott Jernigan, Mike Meyers' CompTIA Security+ Certification Guide, Third Edition (Exam SY0-601) 3rd Edition, ISBN-13: 978-1260473698, ISBN-10: 1260473694, May 4, 2021

[16] Mariam T. Tennoe, Susan F. Henssonow, Padding (Cryptography) Paperback, ISBN-10: 6130363648, ISBN-13: 978-6130363642, Juny 2010

СПИСЪК СЪС СЪКРАЩЕНИЯ

GDPR - General Data Protection Regulation

DNS - Domain Name System

TLD - top-level domain

ARPA - Automatic radar plotting aids

DNNSEC - Domain Name System Security

FTP - File Transfer Protocol

FIPS - The United States' Federal Information Processing Standards

NIST - National Institute of Standards and Technology

API - Application Programming Interface

RSA - Rivest-Shamir-Adleman encryption algorithm

TLS - Transport Layer Security

DKIM - Domain Keys Identified Mail

SMTP - Simple Mail Transfer Protocol

MTA-STS - Mail Transfer Agent Strict Transport Security

SPF - Sender Policy Framework

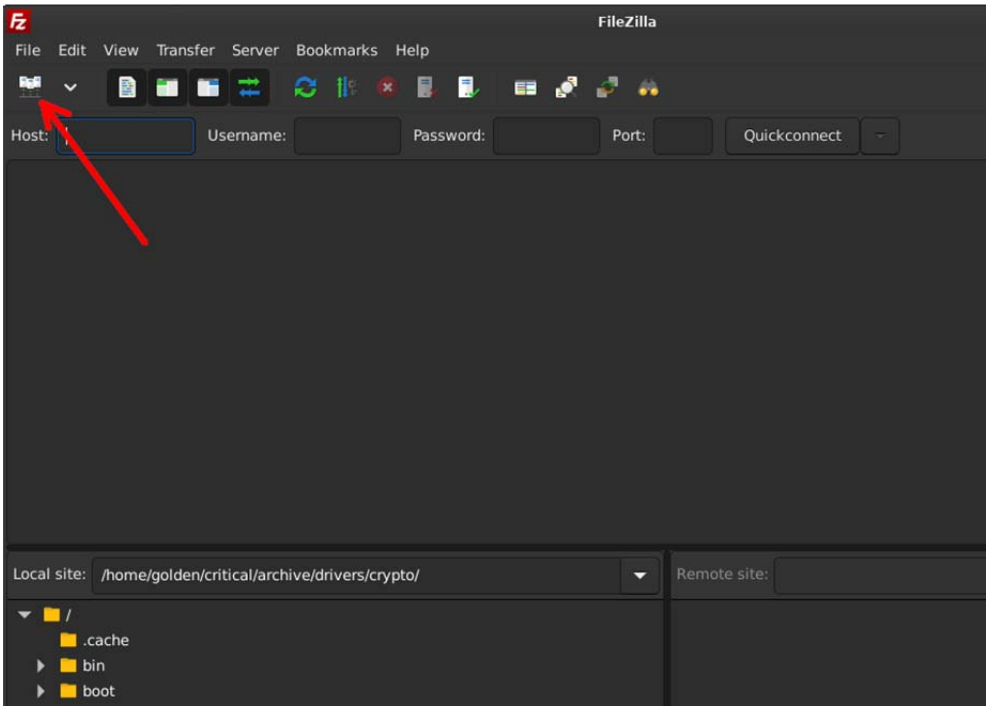
ECDSA - Elliptic Curve Digital Signature Algorithm

ЦСИТУ - Център за споделени ИТ услуги

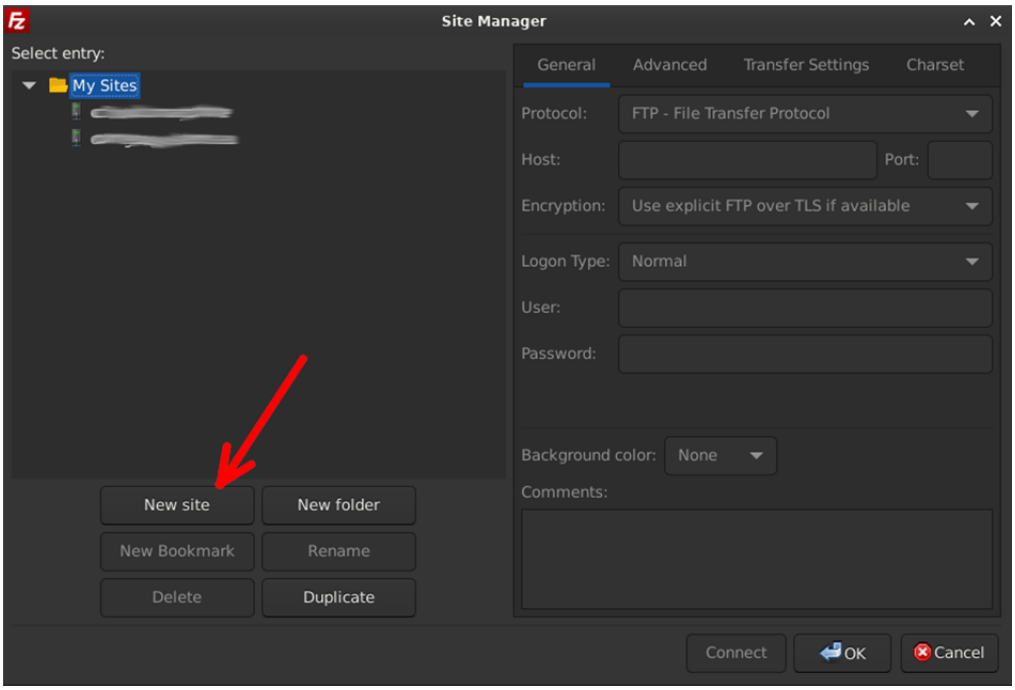
Приложение 1:

Ръководство за конфигуриране на FTP клиент

1. От менюто на FileZilla или от бързата връзка показана на Фиг. 1 се извършва създаване на нова връзка към FTP сайт:

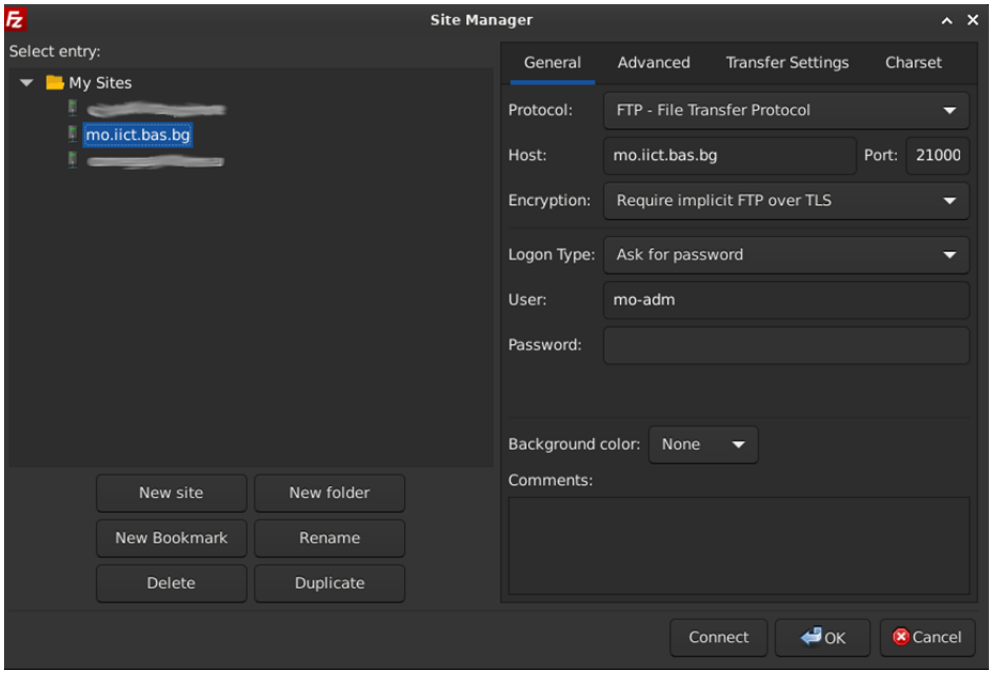


2. От появилия се прозорец Site Manager се избира бутона [New Site], виж фиг. 2:



3. След стъпка 2, дясната страна на екрана на Site manager, менюто се актира и в General се въвежда информацията за FTP сайта към който ще се сварзва клиента. Като в полето Host трябва да се въведе адреса на сайта, до който трябва да се направи връзката. За примера е използван „mo.iict.bas.bg“. За полето Logon Type: се препоръчва да се избере „Ask for password“, което е в съгласие с добрите практики по кибер хигиена. Така паролата ще бъде поискана еднократно от FileZilla клиента и ще бъде „забравена“, след приключване на работа с програмата. При тази опция паролата не се записва в хранилището за пароли на програмата и се избягва риска да бъде атакувана и откраднатa от някой или чрез зловреден софтуер. В полето User се въвежда потребителското име за достъп до услугата, което ще бъде запомнено за улеснение в настройките за този сайт. Останалите настроки, като Protocol, Port и

Encryption, се приемат за статични за сървъра на *.iict.bas.bg и са задължителни, така както са представени на фиг. 3:



Те са, както следва:

Protocol	FTP – File Transfer Protocol
Port	21000
Encryption	Require implicit FTP over TLS

След натискане на [OK] връзката за FTP сайта се запазва. В последствие е възможно да бъде активирана за свързване чрез бутона [Connect] отново от менюто Site Manager.