IT4Sec Reports 148
http://dx.doi.org/10.11610/it4sec.0148

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 2022

Велизар Шаламанов, Иван Благоев, Илиян Илиев, Ниво на зрялост на кибер сигурността на инфраструктурата в домейна iict.bas.bg**,** *IT4Sec Reports 148* (декември 2022), http://dx.doi.org/10.11610/it4sec.0148

IT4Sec Reports 148 „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 148 „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

Съдържание

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 доклад за 2022 г. 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) от 2020 година.

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 „Изследване / оптимизация (Лаборатория) на цифровата трансформация и киберустойчивост“ в ИИКТ-БАН (Зала 2, бл. 25А).

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 2021/2022 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.

Основните постижения, предмет на този доклад са:

- Автоматично блокиране на достъп по IP адрес При опит за ХАКЕРСКА атака на ПОТРЕБИТЕЛСКИ пароли.
- Ежедневен агрегиран статистически доклад за активността на електронната поща
- Система за забавяне на потока от изходяща електронна поща при голям брой писма в опашката

Резултатите по проект „Зора“ бяха представени на Директорски съвет през юли 2022 г. с решение работата по проекта да продължи под ръководството на зам. директора доц. д-р Николай Стоименов като част от изпълнението на Стратегията на ИИКТ до 2030 г., а изследователската част да продължи като бюджетен проект в секция ИТ в сигурността с ръководител доц. д-р Велизар Шаламанов и зам. ръководител гл. ас. Иван Благоев от секция „Моделиране и оптимизация“ с привличане на сътрудници и докторанти на института.

1. АВТОМАТИЧНО БЛОКИРАНЕ НА ДОСТЪП ПО IP АДРЕС ПРИ ОПИТ ЗА ХАКЕРСКА АТАКА НА ПОТРЕБИТЕЛСКИ ПАРОЛИ.

Кибер защитата на услугата за електронна поща е подобрена, чрез система за разкриване и блокиране на хакерски атаки срещу паролите на потребителски акаунти. Начина на действие е, като се регистрира броят неуспешни опити за въвеждане на потребителски парола към услугата за електронна поща. При три неуспешни опита за парола регистрирани от един и същ IP адрес в рамките на деня, се блокира достъпа на този IP адрес на ниво протокол TCP/IP до всички ресурси на сървъра. Правилото за блокиран IP адрес се отменя автоматично след 1 ден.

Услугата електронна поща към домейн iict.bas.bg обслужва **повече от 200 потребителски акаунта**. В организацията липсва централизирано управление на

информационните ресурси. Нивото на обща кибер хигиена сред потребителите също е различно и не се провеждат периодични курсове актуализиращи познанията им (по ННП ИКТ в НОС екипът е разработил по задача 3.2.1. е-обучение по Кибер хигиена, което може да се ползва при решение на Директорския съвет). По тази причина има потребители, които използват не много сложни пароли и вероятно използват една и съща парола за повече от един акаунт за услуги в Интернет. Това прави редица потребителски акаунти особено уязвими за разбиване от хакери. От журналите на системата стана ясно, че често потребителски акаунти към пощенската услуга са подложени на атаки за налучкване на паролата, като се използват dictonary атаки и/или статистически комбинации за съставяне на пароли. Следва извадка от журнала на пощенската услуга към домейна iict.bas.bg:

...

Nov 27 09:37:40 mail postfix/smtps/smtpd[308732]: connect from unknown[5.34.207.94]

Nov 27 09:37:40 mail postfix/smtps/smtpd[308732]: setting up TLS connection from unknown[5.34.207.94]

Nov 27 09:37:42 mail postfix/smtps/smtpd[308732]: Anonymous TLS connection established from unknown[5.34.207.94]: TLSv1.2 with cipher ECDHE-ECDSA-AES256-GCM-SHA384 (256/256 bits)

Nov 27 09:37:48 mail postfix/smtps/smtpd[308732]: warning: unknown[5.34.207.94]: SASL LOGIN authentication failed: authentication failure

Nov 27 09:37:48 mail postfix/smtps/smtpd[308732]: disconnect from unknown[5.34.207.94] ehlo=1 auth=0/1 rset=1 commands=2/3

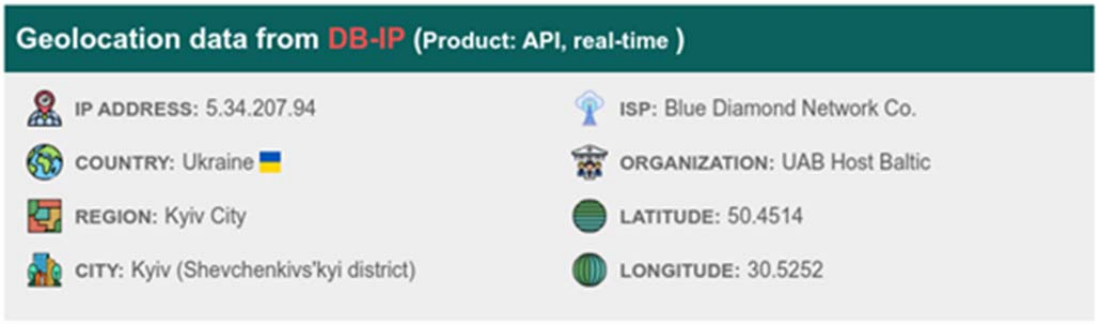
...

От записаното в журнала личи, че IP адрес 5.34.207.94 е искал достъп до ресурсите за изпращане на електронна поща, но е предложил невалидна парола за достъп. Атаки от този вид имат шансове, ако атакуващия може да приложи голям брой опити срещу акаунта на жертвата. Внедрената кибер защита, прави този вид хакерски атаки напълно неефективни.

```
Chain     postfix-sasl (1 references)
target     prot opt source               destination
REJECT     all  --  5.34.207.94          0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.77          0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.58          0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.199         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.198         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.197         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.196         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.195         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.193         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.192         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.191         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.190         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.189         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.186         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.185         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.183         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.153         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.135         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.114         0.0.0.0/0           reject-with icmp-port-unreachable
REJECT     all  --  5.34.207.107         0.0.0.0/0           reject-with icmp-port-unreachable
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Фиг. 1

На фиг.1 е представена снимка на екрана, която показва поредица от блокирани от кибер защитата IP адреси. Всичките IP-та са от един сегмент в поредица и са направили опити за откриване на парола чрез налучкване. Правилото във Firewall е с име postfix-sasl, блокирането на IP адреси, от които са регистрирани действия на кибер атаки. Вероятно атакуващия използва облачна услуга, която може да се наеме от всеки по света и нейната локация е без значение, защото зад определен IP адрес, може да се крие наемател от всяка точка на света. Също така е възможно и да е похитен акаунт на потребител към облачна услуга и този, който атакува всъщност да го прави през сървърни ресурси на съвсем друг човек, който може даже да не подозира, че е станал жертва на хакери. В конкретния случай, според гео локацията на IP адрес 5.34.207.94 се намира облачен хостинг позициониран в град Киев в Украйна (фиг.2):



Фиг. 2

Поредността на IP адресите означава, че те всички са собственост на един и същ доставчик на услугата. Поредността на IP-тата говори, че е възможно хакер да е похитил поредица от сървъри, които дори може да са на един и същ клиент. Съответно хакерът атакува от там пощенската услуга на iict.bas.bg. Но след загуба на връзка от определен IP адрес, заради кибер защитата на iict.bas.bg, продължава със следващия наличен. Докато изчерпва всичките IP адреси с които разполага и губи възможността да използва вероятно похитените машини за още атаки срещу ресурси на iict.bas.bg.

2. ЕЖЕДНЕВЕН АГРЕГИРАН СТАТИСТИЧЕСКИ ДОКЛАД ЗА АКТИВНОСТТА НА ЕЛЕКТРОННАТА ПОЩА

Специализиран софтуер генерира ежедневни доклади, които се извличат чрез записите в системните журнали на услугата за електронна поща. Твърде трудоемко е ежедневно да се преглежда генерираната информация в системните журнали за работата на системата. Информацията е твърде много, а колкото повече потребители, комуникации и активност има даден сървър, става съвсем трудно. За подобряване кибер сигурността и администрирането на услугата са внедрени два специализирани софтуера за анализ и генериране на статистически отчети за работата на услугата електронна поща.

Първото внедрено решение е специализиран софтуер с отворен код, с наименование „pflogsumm“. Функцията му е, да генерира много богата статистическа информация за работата на пощенската услуга (фиг.3):

```
Postfix log summaries for Nov 21

Grand Totals
------------
messages

    356   received
    439   delivered
      0   forwarded
      9   deferred  (10  deferrals)
      0   bounced
    119   rejected (21%)
      0   reject warnings
      0   held
      0   discarded (0%)

  89510k  bytes received
 111530k  bytes delivered
    202   senders
    102   sending hosts/domains
    133   recipients
     19   recipient hosts/domains


Per-Hour Traffic Summary
------------------------
    time          received  delivered   deferred    bounced     rejected
    ------------------------------------------------------------------------
    0000-0100            1          2          0          0            4
    0100-0200            2          2          0          0            0
    0200-0300            5          5          0          0            3
    0300-0400            4          4          0          0            4
    0400-0500            7          7          0          0            1
    0500-0600            6          6          0          0            3
    0600-0700           11         11          0          0            4
    0700-0800            6          8          0          0            3
    0800-0900           11         15          2          0            1
    0900-1000           18         19          0          0            3
    1000-1100           44         65          3          0            3
    1100-1200           35         46          1          0            7
    1200-1300           25         27          0          0           11
    1300-1400           45         65          1          0            8
    1400-1500           32         42          2          0            2
    1500-1600           22         25          0          0            3
    1600-1700           16         17          1          0            4
    1700-1800            7          7          0          0            7
    1800-1900           10         12          0          0           19
    1900-2000           22         24          0          0            9
    2000-2100            6          6          0          0            4
    2100-2200            9         13          0          0           12
    2200-2300            8          8          0          0            4
    2300-2400            4          3          0          0            0
```

Фиг. 3

На фиг.3 е се вижда първата част от отчета и включва обща информация за работата на услугата за последните 24 часа. В началото от „Grand Totals“ става ясно, колко общо писма за електронна поща са обработени за съответния период. Като 119 или 21% от всички писма за 24-те часа на 21 Ноември са били отказани. Тази стойност е много показателна за ефективността на системата за защита на потребителите от непоискана и злонамерена поща. Всяко едно съобщение преминава през поредица от проверки, преди да се достави на потребителя на организацията, като:

- проверка за легитимност на сървъра, който изпраща писмото;
- проверка на легитимността на DNS записите и DKIM подписите към съобщението;
- проверка, дали сървъра изпращащ писмото е включен в черни списъци за лоша репутация;
- проверка от сървърната антивирусна защита за наличието на злонамерен код в писмото;

- проверка на писмото за наличие на елементи отговарящи за непоискана поща – спам;

Ако изпратена електронна поща към iict.bas.bg не успее да премине през всички гореизброени проверки, то се отказва. Причината за получаването на много малко количество на непоискана поща от потребителите и блокирането на 21% от писмата, доказва ефективността на наличните системи за сигурност.

Детайлна статистическа информация за броя на изпращаната поща, времето за обработка от сървъри, както и други домейни с пощенски услуги се извежда от „Host/Domain Summary: Message Delivery“:

```
Host/Domain Summary: Message Delivery
---------------------------------------
 sent cnt  bytes   defers   avg dly max dly host/domain
 -------- -------  -------  ------- ------- -----------
    355    63916k       0     3.1 s    1.9 m  iict.bas.bg
     25    20128k       0     4.8 s    1.1 m  gmail.com
     21    11298k       0     3.8 s   39.0 s  abv.bg
      8   508526        8     6.9 m    9.0 m  isdip.bas.bg
      6   268214        0     6.1 s    8.9 s  tu-sofia.bg
      4   136338        0     0.8 s    0.9 s  ilchev.net
      3   193546        0     5.0 s    7.5 s  bas.bg
      3    39993        0    18.7 s   22.0 s  lml.bas.bg
      2     1032k       2     7.5 m    7.8 m  iit.bas.bg
      2    18846        0     1.8 s    1.9 s  parallel.bas.bg
      2     9162        0     1.2 s    1.3 s  vfu.bg
      1    13597k       0    22.0 s   22.0 s  mail.bg
      1   330706        0     6.8 s    6.8 s  fmi.uni-sofia.bg
      1    77063        0     6.6 s    6.6 s  me.com
      1     3513        0     6.2 s    6.2 s  mdpi.com
      1     3055        0     6.3 s    6.3 s  cys.bg
      1     2136        0     6.3 s    6.3 s  redesign.bg
      1     1641        0     0.4 s    0.4 s  ir.bas.bg
      1     1641        0     0.8 s    0.8 s  biomed.bas.bg
```

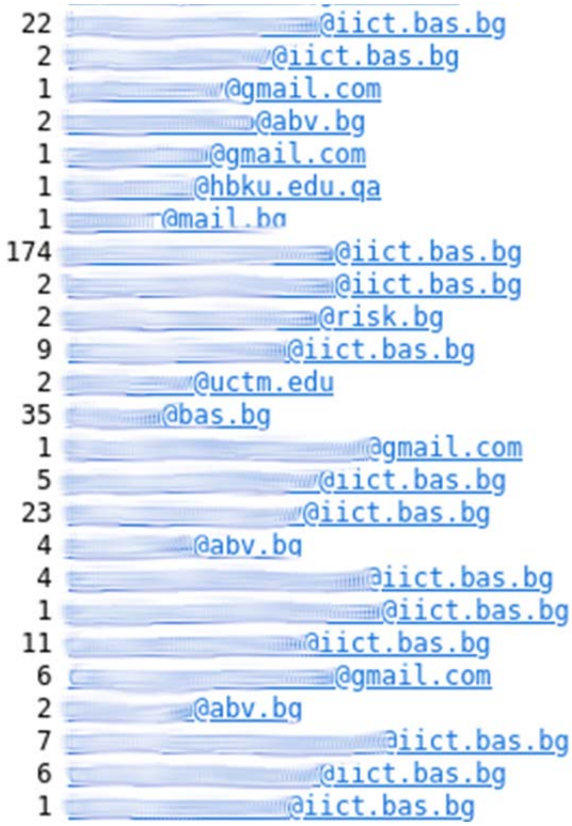
Фиг. 4

Останалите данни в разглеждания отчет са:

- Host/Domain Summary: Messages Received – статистическа обобщена информация за получените съобщения;
- Senders by message count – статистическа агрегирана справка за брой на писмата според изпращачи;
- Recipients by message count - статистическа агрегирана справка за брой на писмата според получатели;
- Senders by message size - статистическа агрегирана справка за брой на съобщенията според изпращачи по обем на писмата;
- Recipients by message size - статистическа агрегирана справка за брой на съобщенията според получателите по обем на писмата;
- Messages with no size data – писма, които не са доставени поради възникнали комуникационни грешки;
- smtp delivery failures – писма отказани от сървъра на трета страна (ако има);

- Fatal Errors: - критични грешки възникнали при комуникация с трети страни или вътрешни по работата на системата (ако има);
- Panics: - други видове критични съобщения свързани с работата на системата (ако има);
- Master daemon messages – системни грешки, които може да възникнат при вътрешната комуникация между отделните услуги (ако има).

Следващото внедрено решение за анализ на системния журнал на пощенските услуги е разработено и внедрено от нашия екип. Целта е да събере и представи в списък потребителите на домейна и общия брой писма, които са изпратили в рамките на деня и на седмична база. Тази статистическа информация заедно с представените отчети от „pflogsumm“, са от ключово значение за откриване на похитени пощенски акаунти на потребители. В първия отчет стойностите на различните справки се увеличават значително и се появяват множество домейни, които не присъстват в обичайната дейност на потребителите. Вторият отчет позволява да се разбере, кой потребител изпраща необичайно големи количества електронна поща. На фиг.5 е представена една малка част от този отчет, където се вижда колко писма са изпратени от дадена кутия за електронна поща:



Фиг. 5

Ако активността и броят на писмата е твърде висок спрямо обичайният за потребител, то става ясно, че пощенският акаунт е похитен. Следователно се използва от злонамерен софтуер (вирус) или е под контрола на хакер. Тъй, като информацията от отчетите е навременна, често и потребителя все още не е разбрал, че акаунта му е похитен. Навременното откриване на проблема и навременните действия водят до ефективното отстраняване на същия. Закъснялата реакция би могла да нанесе вреда на услугите

свързани с домейна и останалите му потребители. Към момента има случай, при който чрез двете системи за генериране на справки от системните журнали, е открит заразен от компютърен вирус потребителски компютър. Вирусът започва да препраща електронна поща, като е прихванал незабелязано акаунта с който потребителя работи на същата компютърна система. Благодарение на получената навременна информация, потребителя е предупреден и акаунта му за електронна поща бе блокиран на време до отстраняване на вируса от компютърната му система.

3. СИСТЕМА ЗА ЗАБАВЯНЕ НА ПОТОКА ОТ ИЗХОДЯЩА ЕЛЕКТРОННА ПОЩА ПРИ ГОЛЯМ БРОЙ ПИСМА В ОПАШКАТА

При натрупване на писма в опашката на пощенската услуга е внедрена система, която изпраща писмата последователно с дефинирано забавяне между тях. Не е необходимо множеството писма от електронната поща да са от зловредни действия, за да се натрупат наведнъж в опашката на услугата. Възможно е да се случат от потребителска активност, която да е по стечение на обстоятелствата. В този случай, ако пощенската услуга започне да залива с писма друга система (на трета страна), е възможно високата активност да се приеме за зловредно действие. Което ще доведе до автоматичното блокиране на получаването на писма от този домейн и вписването му в черен списък за пощенски сървъри с лоша репутация. Не е страшно да се изпращат много писма по електронната поща, опасно е ако се изсипват в голямо количество за малко време. Това би могло да доведе до блокирането на сървъри, които са с по-слаб капацитет и по-бавна Интернет свързаност от iict.bas.bg. По тази причина, такива действия се смятат за „враждебни“ и водят до санкциониране чрез блокиране от множество сървъри по света.

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

Направените подобрения в кибер сигурността и устойчивостта на услугите към домейн iict.bas.bg по проект Зора, дадоха незабавни положителни резултати. Покриването на целите по задачите в този проект са доказателство, че е възможно да се достига до сравнително качествени и добре защитени услуги и с малки бюджети. Като могат да се покриват нуждите на организация с няколко стотин човека потребители. Трябва да се има в предвид, че експертизата и опита могат да покрият голяма част от необходимостите с минимални средства при съчетаване на административните задачи с изследователската работа (особено за докторантите), но истински качествени и устойчиви критични услуги, не могат да се изграждат с редица компромиси при липсата на надеждна технологична инфраструктура и професионално ангажиран персонал.

Работата по Проект Зора се поддържа от редица докторантски изследвания:

1. Преминаване от управление на ресурси към управление на услуги (Илиян Илиев);
2. Развитие на цифрови компетентности в подкрепа на цифровата трансформация и киберусройчивост (Силвия Матерн);

3. Виртуализация и сигурност при създаване на облачни решения за ИКТ услуги (Антония Гогова);
4. Повишаване на киберсигурността с криптографски методи и др.
5. Обвързването на докторантските изследвания с реални проблеми на цифровата трансформация на примера на ИИКТ ще позволи въвеждане на оптимизирани процеси по:
6. Стратегическо планиране на информационните ресурси и услуги;
7. Управление на промяната в е-Инфраструктурата и Сигурността;
8. Управление на Каталога от ИТ услуги;
9. Управление на иновациите в е-Инфраструктурата и Сигурността;
10. Развитие на партньорството за разширяване на е-Инфраструктурата и Сигурността;
11. Бизнес планиране за е-Инфраструктурата и Сигурността;
12. Одит и повишаване на нивото на зрялост на е-Инфраструктурата и Сигурността.

Разделянето на проект „Зора“ от 2023 г. на два проекта – изследователски по оптимизация на цифровата трансформация (и кибер устойчивост в сложно организации) и административен по изпълнение на Стратегията на ИИКТ до 2030 ще позволи и надеждно финансиране на втория, вкл. чрез механизми като Националния План за Възстановяване и Устойчивост, а на първия по Оперативна **Програма** за **научни изследвания**, иновации и дигитализация за интелигентна трансформация.

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, I SBN-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