ПРИЛОЖЕНИЕ НА ДОБРИТЕ ПРАКТИКИ ЗА ЗАЩИТА НА ИНТЕРНЕТ ИНФРАСТРУКТУРАТА НА ВИСШИТЕ УЧИЛИЩА В БЪЛГАРИЯ

Ас. Юрий Кузнецов, y.kuznetsov@uni-svishtov.bg
Катедра "Бизнес информатика"
Стопанска Академия "Д. А. Ценов" – Свищов

Резюме: Комуникационната инфраструктура на висшите училища е цел на постоянно увеличаващи се и променящи своя тип атаки и заплахи. Прилагането на добрите практики на защита на публичната информационна инфраструктура води до повишаване на нейната сигурност и осигурява ефикасна защита на данните. Направеният анализ на приложението на тези практики във висшите училища в България показва, че не се обръща необходимото внимание на информационната сигурност в този тип организации.

Ключови думи: информационна сигурност, висше училище, защита на комуникациите

JEL:D80

IMPLEMENTATION OF BEST PRACTICES OF A PROTECTION OF INTERNET INFRASTRUCTURE OF THE HIGH SCHOOLS IN BULGARIA

Assist. Prof. Yuriy Kuznetsov, y.kuznetsov@uni-svishtov.bg
Department of Business Informatics
D.A.Tsenov Academy of Economics – Svishtov

Abstract: The communications infrastructure of universities is a target of constantly increasing and new in type attacks and threats. The implementation of best practices of protection of the public information infrastructure leads to increasing its security and provides effective data protection. The analysis of the implementation of these practices at universities in Bulgaria shows that adequate attention to information security in this type of organizations has not been paid.

Keywords: information security, higher education, protection of communications

JEL:D80

ПРИЛОЖЕНИЕ НА ДОБРИТЕ ПРАКТИКИ НА ЗАЩИТА НА ИНТЕРНЕТ ИНФРАСТРУКТУРАТА НА ВИСШИТЕ УЧИЛИЩА В БЪЛГАРИЯ

Ас. Юрий Кузнецов, y.kuznetsov@uni-svishtov.bg
Катедра "Бизнес информатика"
Стопанска Академия "Д. А. Ценов" – Свищов

Увод

Прилагането на добрите практики за защита на информацията трябва да е приоритет на управлението на всяка организация, независимо от отрасъла, в който тя функционира. Висшите училища не трябва да правят изключение от това правило. Обект на изследването е Интернет инфраструктурата на висшите училища в България. Предмет на изследването е защитата на Интернет

инфраструктурата на висшето училище чрез използването на сигурни и добре конфигурирани комуникационни протоколи. Изграждането на защитена и надеждна комуникация допринася не само за по-високо ниво на сигурност и доверие на потребителите към предлаганите от висшето училище услуги, но и повишава защитата срещу атаки към вътрешната информационна инфраструктура. Изследването има за цел да анализира причините за атаки към информационните ресурси във висшите училища и как е защитена Интернет инфраструктурата, чрез която висшето училище комуникира с клиентите си (кандидат-обучаеми и потребители на образователен продукт). За нуждите на изследването, чрез използване на различни софтуерни инструменти, са направени анализи, чрез които е измерено как са приложени добрите практики за изграждане на защитени Интернет комуникации във висшите училища в България.

1. Необходимост от защита на информационна инфраструктура на висше училище

В последните години се забелязва тенденция за увеличение на пробивите на сигурността във висшите училища. Информационните системи на едно висше училище (ВУ) са привлекателни мишени за хакерите, защото не съдържат само финансови и лични данни, но също така съдържат и ценна интелектуална собственост. Тези заплахи принуждават академичните среди да направят преоценка на начина, по който се съхраняват и защитават огромни регистри от информация, често намиращи се в децентрализирани компютърни мрежи достъпни за хиляди студенти, преподаватели и изследователи. Старши съветникът на SecuriCore, проект за информационна сигурност в университета в Индиана, Питърсън препоръчва моделът на информационна сигурност да бъде по-затворен, по-скептичен и по-циничен (Calvert , 2014). Точно както в кампусите са поставени железни врати, охрана и камери за наблюдение през последните десетилетия, така може да се реши да се сложи край на ерата на свободния достъп до онлайн ресурси. По наше мнение, това е доста апокалиптична картина, но официалните данни за пробиви и мащабите за компрометираните данни в университетски информационни системи впечатляват (Chronology of Data Breaches, н.д.):

- 3-ти март 2017 – Откраднати са данни за над 6,6 милиона избиратели от мрежата на университета в Kennesaw Джорджия.
- 2-ри март 2017 – Откраднат е лаптоп на преподавател в университета в Санта Круз, съдържащ данни за студенти.
- 13-ти февруари 2017 – Списък с лични данни за студенти в колежа Platt Калифорния е изпратен на грешен е-мейл адрес.
- 18-ти ноември 2016 – Разбита е база от данни, съдържаща над 400 000 записа със студентски данни в университета в Мичиган.
- 6-ти март, 2014 - Университетът в North Dakota уведомява студенти, служители и преподаватели, че 290 780 лични записи, включително номера на социални осигуровки, в нарушение на правилата, са били публично изложени на нерегламентиран достъп.
- 26-ти февруари, 2014: Университета в Indiana по погрешка излага на публичен достъп лични данни, включително номера на социални осигуровки, на 146 000 студенти и възпитаници.

Преди въвеждането през 2018 година на Регламент (ЕС) 2016/679 „Регламент за защита на физическите лица по отношение на обработката на лични данни и за свободното движение на такива данни и за отмяна на Директива 95/46 / ЕО“ администраторите на лични данни в Европейския съюз нямаха задължението да информират за пробиви в сигурността и изтичане на лични данни, но по наше мнение няма основание да се смята, че такива пробиви във висши училища в Европа са рядкост и с по-малко на брой засегнати лица.

Причините за увеличаване на атаките към висшите училища могат да се търсят в следните направления:

- **Промяна на типа на атаките**. Предоставянето на готови мрежи от заразени компютри (botnet) за нуждите на рекламата, онлайн гласуване (Скандал с Мис България - отнеха титлата на Ина Манчева, н.д.), обработка (Botcoin: Bitcoin Mining by Botnet, н.д.) съхранение и разпространение на данни, атакуване на други компютри и т.н. се превръща през последните години в доходоносен бизнес (Malware-as-a-service) (‘Malware-as-a-service’ Market Booms as Prices for Malware and Botnet Creation Tools Decline, н.д.). Предоставят се цели мрежи от заразени компютри (10000 до 100000) за определен период от време срещу определена сума. През 2007, създателят на TCP/IP протокола В. Сърф, прави изказване че около 100-150 милиона (!), от общо 600 милиона компютри свързани в Интернет, са заразени с някакъв зловреден софтуер. Оказва се, че съвременните вируси и троянски коне освен с цел изтриване, кражба или промяна на данни имат за предназначение да получат достъп до системата, нейното отдалечено управление и последващата възможност тя да бъде използвана за последваща масирана атака. Академичните мрежи разполагат с голям брой компютри и може да се каже неограничен по скорост и капацитет Интернет достъп, което ги прави интересни за нуждите на изграждането на големи по обем мрежи от „зомбирани“ компютри.
- **Ниско ниво на сигурност на части на компютърните мрежи.** Във висшите училища локалната мрежа най-често бива сегментирана на пет части: сегмент обслужващ нуждите на управлението (за счетоводна, финансова, кадрова и друга информация); сегмент за управление на информацията за обучаемите (канцеларии и факултети); научноизследователски сегмент на мрежата (в него се намират и работните места на преподавателите); сегмент в който се намират компютърните и мултимедийни зали и лаборатории; сегмент за безжичен достъп. В сегментите за изследване, обучение и сегмента за безжичен достъп (използвани от обучаеми, научни работници и преподаватели) се смята, че всякакъв род ограничения вреди. Също така се смята, че няма важни данни, които са от съществено значение и не трябва да се предприемат специални действия по тяхната защита. Често нивото на защита на тези сегменти е близко до нивото на защита на едно Интернет кафе. Може да се каже, че спазвайки неутралитет и не обръщайки внимание на проблемите за защита на изследователската част на своите мрежи доста университети се превръщат в места удобни за извършване на компютърни престъпления или спомагат за това.
- **Наличие на голямо количество интелектуална собственост в дигитален вид.** Наред с интелектуални продукти създадени за нуждите на обучение и в реализацията на различни научно-

изследователски проекти, във висшето училище се намират множество продукти на интелектуален труд в електронна форма, така например: книги и списания; абонаменти за достъп до бази данни и електронни библиотеки; серийни номера и лицензи и т.н. През 2011 става известен случая с Аарон Шварц, който е арестуват в MIT за нерегламентиран достъп до огромен брой научни статии и данни в онлайн ресурса Scopus, за който университета има пълен и безлимитен достъп. В резултат на което, съдът го признава за виновен в 11 нарушения на Закона за компютърни измами и злоупотреби и го наказва с глоба от един милион долара и 35 години затвор (Alleged hacker charged with stealing over four million documents from MIT network, 2011)!

- **Наличие на големи по обеми лични и корпоративни данни.** Не на последно място трябва да се отбележи, че наличието на големи по обем лични данни и данните за партньорите (физически и юридически лица) на висшето училище също е важна причина за интереса на злоумишлените атакуващи. За нуждите на различни видове анализи свързани с повишаване на качеството на процесите и развитие на общности на бивши възпитаници, данните за студентите не се архивират, а се държат „живи“. Също така, при извършване на научно-изследователска дейност в академичните мрежи се намират данни за здравословното състояние на пациенти (за медицинските ВУ), финансови данни и икономически показатели за фирми или организации и т.н.

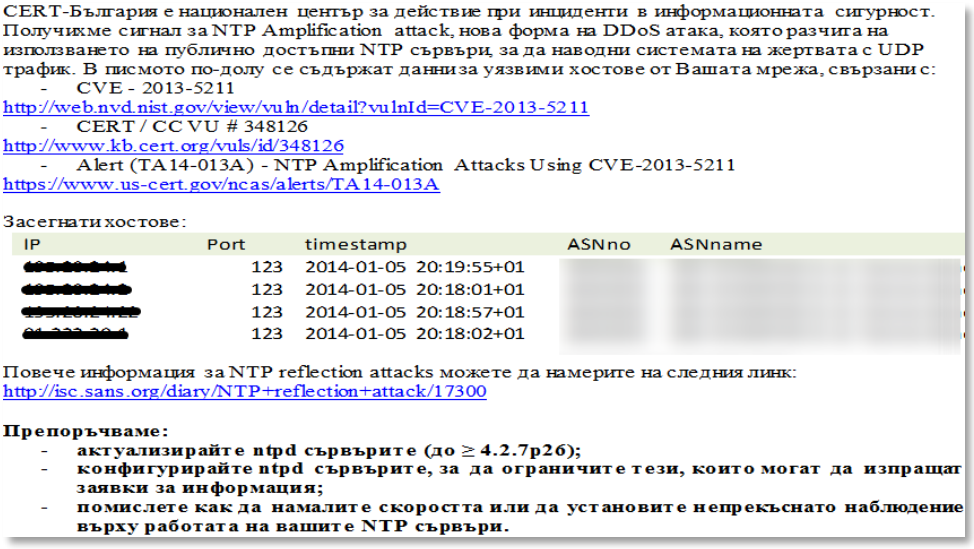
Защита на данните и информацията на дадено висше училище може да бъде структурирана в следните направления:

- спазване на законови и нормативни изисквания;
- опазване на собствената интелектуална собственост;
- осигуряване на непрекъснатост на процесите;
- имидж на висшето училище.

В България няма специализирано законодателство за областта на образованието свързано с класифицирането на данните и начините за тяхната обработка и съхранение и поради тази причина, учебните заведения се съобразяват с по-широкото законодателство, като например Законът за защита на личните данни при осигуряване на информационната сигурност. Тълкуването на по-широко законодателство изисква добра юридическа подготовка на юридическите консултанти на висшите училище и води до различни практики и тълкувания във всяко учебно заведение. Липсата на дефиниране на данните и тяхното класифициране силно затруднява прилагането на адекватни мерки за тяхната защита. Например, в САЩ има специално законодателство свързано със съхраняването на данни в учебни заведения (училища и колежи) (Family Educational Rights and Privacy Act (FERPA)). Дефинирани са точно типът на данните, начините за даване на съгласие за съхранение, периодите за съхранение, правата за достъп до данните и начините за тяхното предоставяне на външни институции .

При класическите анализи на риска свързан със защита на данните се фокусира вниманието върху това доколко една организация е защитена от външни атаки, и доколко данните в дадената организация са предпазени. С добавянето на термина „споделяне на отговорност” може да се каже, че защитата на данните придобива нови измерения. Нивото на защита трябва да се повиши и в онези места, на които до този момент не е било обръщано внимание. Смята се,

че когато някой се свързва в Интернет той трябва да спазва правилата на една общност и да не извършва действия застрашаващи сигурността на другите. Доста юристи считат, че вината на посредниците не трябва да се омаловажава. Това означава автоматично, че бездействието (в случая неправилна конфигурация, настройка, заразен компютър и т.н.), застрашаващо другите в Интернет, също може да се разглежда като заплаха. Това налага реализирането на политики за сигурност обърнати не само в посока на защита на данните и информацията на самата организация, а и изследване и предотвратяване на атаки от самата научноизследователска организация насочена към външния свят. Не трябва да бъдат игнорирани по никакъв начин предупреждения за нарушения на сигурността (вж. фиг. 1) или авторските права (вж. фиг. 2) от вътрешността на дадено висше училище.



CERT-България е национален център за действие при инциденти в информационната сигурност. Получихме сигнал за NTP Amplification attack, нова форма на DDoS атака, която разчита на използването на публично достъпни NTP сървъри, за да наводни системата на жертвата с UDP трафик. В писмото по-долу се съдържат данни за уязвими хостове от Вашата мрежа, свързани с:

- CVE - 2013-5211

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5211

- CERT / CC VU # 348126

http://www.kb.cert.org/vuls/id/348126

- Alert (TA14-013A) - NTP Amplification Attacks Using CVE-2013-5211

https://www.us-cert.gov/ncas/alerts/TA14-013A

Засегнати хостове:

IP	Port	timestamp	ASNno	ASNname
[redacted]	123	2014-01-05 20:19:55+01		
[redacted]	123	2014-01-05 20:18:01+01		
[redacted]	123	2014-01-05 20:18:57+01		
[redacted]	123	2014-01-05 20:18:02+01		

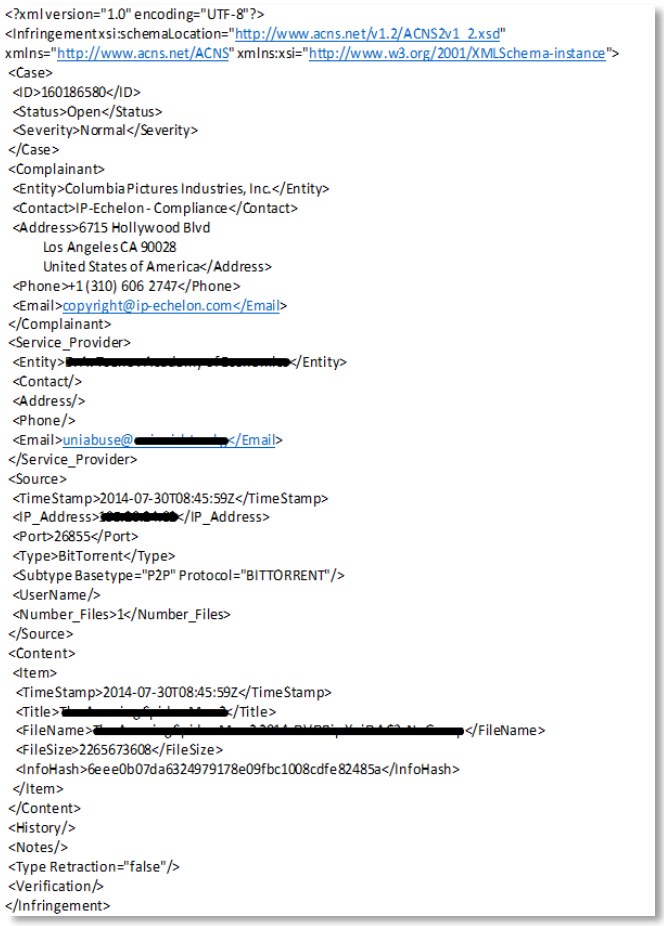
Повече информация за NTP reflection attacks можете да намерите на следния линк:
http://isc.sans.org/diary/NTP+reflection+attack/17300

Препоръчваме:

- **актуализирайте ntpd сървърите (до ≥ 4.2.7p26);**
- **конфигурирайте ntpd сървърите, за да ограничите тези, които могат да изпращат заявки за информация;**
- **помислете как да намалите скоростта или да установите непрекъснато наблюдение върху работата на вашите NTP сървъри.**

Фигура 1. Предупреждение за проблеми със сървъри, които могат да бъдат използвани за атака на външни ресурси

Висшите училища имат особен статут от гледна точка на държавната администрация и предоставянето на услуги. От една страна, държавните висши училища имат задължението да обменят голям обем данни с различни държавни институции, а от друга - не са задължени да спазват изискванията на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност . В последното изменение на наредбата от 2013 (член 2 (2)) в пожелателна форма е казано, че изискванията на наредбата могат да бъдат приложени и към организации осъществяващи публични услуги: „(2) Прилагането на разпоредбите на глава трета и използването на информационни системи, удостоверени по реда на наредбата, могат да се прилагат от лицата, осъществяващи публични функции и от организациите, предоставящи обществени услуги.“. Поради тази причина, в настоящия момент няма нито едно висше учебно заведение имащо сертификация за управление на информационната сигурност, в съответствие с международния стандарт ISO 27001:2005, което е изискване на наредбата. По наше мнение, изискванията на този стандарт са трудно реализуеми в едно висше училище, но от друга страна, използването на добрите практики на стандарта, би било ползотворно за изграждането на системи за информационна сигурност в учебното заведение.



```
<?xml version="1.0" encoding="UTF-8"?>
<Infringement xsi:schemaLocation="http://www.acns.net/v1.2/ACNS2v1_2.xsd"
xmlns="http://www.acns.net/ACNS" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <Case>
  <ID>160186580</ID>
  <Status>Open</Status>
  <Severity>Normal</Severity>
 </Case>
 <Complainant>
  <Entity>Columbia Pictures Industries, Inc.</Entity>
  <Contact>IP-Echelon - Compliance</Contact>
  <Address>6715 Hollywood Blvd
        Los Angeles CA 90028
        United States of America</Address>
  <Phone>+1 (310) 606 2747</Phone>
  <Email>copyright@ip-echelon.com</Email>
 </Complainant>
 <Service_Provider>
  <Entity>[redacted]</Entity>
  <Contact/>
  <Address/>
  <Phone/>
  <Email>uniabuse@[redacted]</Email>
 </Service_Provider>
 <Source>
  <TimeStamp>2014-07-30T08:45:59Z</TimeStamp>
  <IP_Address>[redacted]</IP_Address>
  <Port>26855</Port>
  <Type>BitTorrent</Type>
  <Subtype Basetype="P2P" Protocol="BITTORRENT"/>
  <UserName/>
  <Number_Files>1</Number_Files>
 </Source>
 <Content>
  <Item>
   <TimeStamp>2014-07-30T08:45:59Z</TimeStamp>
   <Title>[redacted]</Title>
   <FileName>[redacted]</FileName>
   <FileSize>2265673608</FileSize>
   <InfoHash>6eee0b07da6324979178e09fbc1008cdfe82485a</InfoHash>
  </Item>
 </Content>
 <History/>
 <Notes/>
 <Type Retraction="false"/>
 <Verification/>
</Infringement>
```

Фигура 2 Предупреждение за нарушение на авторски права

Защитата на наличната интелектуална собственост във висшето училище поставя високи изисквания към управлението на информационната сигурност - точното класифициране на ресурсите и носителя на права и възможностите за тяхното разпространение (продажба). Преминава се от системите за пълен достъп до всичко, защото е финансирано с публичен ресурс до пълното блокиране на всичко, защото е финансирано със собствени средства и е инвестирано лично време. Достига се до крайности, при които не се осигурява достъп до учебни планове и програми на дисциплини. Внедряването на системи за борба с плагиатството също довежда до лавинообразно увеличаване на дигиталните ресурси в едно висше училище.

Поддържането на високо ниво на информационна сигурност е свързано с осигуряването на процеса по непрекъснатост на бизнес процесите във висшето училище. Съвременното иновативно висше училище има високо ниво на автоматизация на процесите и наличие на голям брой клиенти изискващи непрекъснат достъп до електронни ресурси за обучение. Вграждането на елементи на оценка на оперативния риск, управлението на непрекъснатостта и други бизнес практики са важен елемент за осигуряване на функционирането на системата като цяло. Например, проблеми с достъпността до информационния уеб сайт по време на кандидатстудентската кампания биха довели до сериозен проблем с имиджа на училище и отлив на кандидати. Поради тази причина, в настоящия момент на повечето висши училища се налага да имат повече от един доставчик на Интернет услуги и е необходимо да се предлага достъп и чрез

протокола IPv6 до ресурсите на учебното заведение. Комуникациите трябва да се осъществяват чрез защитени протоколи.

2. Анализ на прилагането на добрите практики при осигуряване на защита на комуникациите

Иновативното ВУ е немислимо без качествена връзка до Интернет за нуждите на обучението и научноизследователската дейност. Обучаемите трябва да имат осигурен качествен дистанционен достъп до ресурси за обучение и различни административни услуги предоставяни от висшето училище. Затова е препоръчително висшето училище да разполага с минимум два доставчика на Интернет и връзка по IPv4 и IPv6. За по-добро управление на трафика и използване на динамични протоколи за маршрутизиране (BGP), добра практика е ВУ да разполага със собствено адресно пространство и собствена автономна система (AS). За проверка на прилагането на добрите практики е проведено изследване на мрежите на висшите училища в България, при осъществяването на което са използвани инструменти за IP сканиране и информацията от регионалния за Европа Интернет регистър RIPE. Направеният анализ (вж. Таблица 1) показва, че само две висши училища удовлетворяват тези изисквания за надеждност.

Таблица 1

Начин на Интернет свързаност на ВУ в България.

Висше училище	**Собствена автономна система**	**Собствено (PI) адресно пространство**	**IPv6 достъп до основния сайт**
Американски университет www.aubg.edu	AS3264	Да	Не
Русенски университет www.uni-ruse.bg	AS48155	Да	Да
Софийски университет www.uni-sofia.bg	AS5421	Да	Да
Университетът по библиотекознание и информационни технологии www.unibit.bg	няма	няма	Не
Стопанска академия – Свищов www.uni-svishtov.bg	AS41352	Да	Не
Висше транспортно училище www.vtu.bg	няма	няма	Не
Медицински университет – Плевен www.uni-pleven.com	няма	няма	Не
Нов български университет student.nbu.bg	AS44805	Да	Не
Медицински университет – Пловдив meduniversity-plovdiv.bg	няма	няма	Не
УНСС www.unwe.bg	няма	няма	Не
Технически университет – София www.tu-sofia.bg	AS28949	Да	Не
Пловдивски университет uni-plovdiv.bg	няма	няма	Не
Икономически университет – Варна www.ue-varna.bg	няма	няма	Не

Югозападен университет www.swu.bg	няма	няма	Не
Великотърновски университет www.uni-vt.bg	няма	няма	Не
Технически университет – Габрово www.tugab.bg	няма	няма	Не
Технически университет – Варна www.tu-varna.bg	AS47174	Да	Не
Медицински университет – София mu-sofia.bg	няма	няма	Не
Медицински университет – Варна mu-varna.bg	няма	няма	Не
УАСГ uacg.bg	AS16328	Да	Не
Минно-геоложки университет mgu.bg	няма	няма	Не
Химикотехнологичен и металургичен университет www.uctm.edu	AS31011	Да	Не
Университет "Проф. д-р Асен Златаров" www.btu.bg	няма	няма	Не
Варненски свободен университет www.vfu.bg	няма	няма	Не

Източник: Оценката е проведена на 9.05.2018.

Изборът на подходяща защита на мрежовите протоколи е от съществена важност за надеждността на цялостната архитектура. Защитата на протоколите е в пряка връзка със заложените минимални изисквания към механизмите за криптография в логическата архитектура. Всички протоколи за защита на XML съобщенията (XML Encryption, XML Signature, XKMS, SOAP Extensions, S2ML, SAML, WS-Security, XACML) разчитат на транспортен протокол, за да осъществят прехвърляне на данни между клиента и сървъра. Препоръчително е да се предвиди използването на защитен транспортен протокол. На съвременния етап на развитие, HTTPS (защитената спецификация на HTTP) е основният протокол за осъществяването на тази задача. През последните години се наблюдават множество пробиви в сигурността при реализирането на този протокол. Непознаването на проблемите и неправилното конфигуриране на сървърите за използването на HTTPS може да доведе до фалшивото усещане за сигурност.

Правилното използване на HTTPS при изграждането на защитена архитектура във ВУ се явява сериозно предизвикателство. Проучване на използваните цифрови сертификати в сайтовете на водещите ВУ в България показва непознаване на добрите практики и произтичащите от това рискове (Вж. Таблица 2 и Таблица 3). С цел проследяване на напредъка при прилагането на HTTPS са направени два анализа: през 2016г. и през 2018г. Анализът през 2018 година показва, че има подобряване на ситуацията, но все още има проблеми при прилагането на защитени протоколи. Някои университети използват безплатния издател на сертификати Let’s Encrypt, което по наше мнения носи определени рискове. Все още се забелязва, че независимо от наличие на сертификати, те не са правилно конфигурирани и сайтовете са уязвими за различни видове атаки. Поради тази причина, препоръчваме при изграждането на портали за електронно обучение и информационни портали свързани с публикуването на лични данни

да се спазват добрите практики, свързани с поддръжка на цифрови сертификати, например ръководството „SSL and TLS Deployment Best Practices“ (SSL and TLS Deployment Best Practices, 2016).

Таблица 2
Оценка на цифровите сертификати за защита на ВУ в България през 2016 година.

Уеб портал	Вид на сертификата	Издател на сертификата	Обща оценка
www.aubg.edu	RSA 2048 bits	DigiCert SHA2 High Assurance Server CA	**A+**
www.uni-ruse.bg	RSA 4096 bits	COMODO RSA Domain Validation Secure Server CA	**A+**
www.uni-sofia.bg	RSA 2048 bits	GeoTrust SSL CA - G3	**A**
www.unibit.bg	RSA 2048 bits	COMODO RSA Domain Validation Secure Server CA	**A**
www.uni-svishtov.bg	RSA 2048 bits	COMODO RSA Domain Validation Secure Server CA	**B**
www.vtu.bg	RSA 4096 bits	RapidSSL CA	**B**
www.uni-pleven.com	Сертификат за www.emretoys.com		**T/B**
student.nbu.bg	RSA 2048 bits	RapidSSL SHA256 CA - G3	**C**
meduniversity-plovdiv.bg	Сертификат за *.superhosting.bg		**T/C**
www.unwe.bg	RSA 4096 bits	RapidSSL SHA256 CA - G3	**F**
priem.tu-sofia.bg	RSA 1024 bits Изтекъл преди година и 9 месеца!	Self-signed	**F**
uni-plovdiv.bg	RSA 2048 bits	GlobalSign Organization Validation CA	**F**
ksp.ue-varna.bg	RSA 2048 bits	Self-signed	**F**
www.swu.bg	RSA 4096 bits	COMODO RSA Domain Validation Secure Server CA	**F**
www.uni-vt.bg,	Липса поддръжка на протокол за защитена връзка		
www.tugab.bg	Липса поддръжка на протокол за защитена връзка		
www.tu-varna.bg	Липса поддръжка на протокол за защитена връзка		
mu-sofia.bg	Липса поддръжка на протокол за защитена връзка		
mu-varna.bg	Липса поддръжка на протокол за защитена връзка		
uacg.bg	Липса поддръжка на протокол за защитена връзка		
mgu.bg	Липса поддръжка на протокол за защитена връзка		
dl.uctm.edu	Липса поддръжка на протокол за защитена връзка		
www.btu.bg	Липса поддръжка на протокол за защитена връзка		
www.vfu.bg	Липса поддръжка на протокол за защитена връзка		

Източник: Използван е анализатор за оценка на ssl сертификати https://www.ssllabs.com/ssltest/analyze.html. Оценката е проведена на 7.08.2016

Таблица 3
Оценка на цифровите сертификати за защита на ВУ в България през 2018 година.

Уеб портал	Вид на сертификата	Издател на сертификата	Обща оценка
www.aubg.edu	RSA 2048 bits	DigiCert SHA2 High Assurance Server CA	**A+**
www.uni-ruse.bg	RSA 4096 bits	COMODO RSA Domain Validation Secure Server CA	**A+**
www.uni-sofia.bg	RSA 2048 bits	GeoTrust SSL CA - G3	**A**
www.unibit.bg	RSA 2048 bits	COMODO RSA Domain Validation Secure Server CA	**A**
www.uni-svishtov.bg	RSA 2048 bits	COMODO RSA Domain Validation Secure Server CA	**B**

www.vtu.bg	RSA 4096 bits	RapidSSL CA	**A**
www.uni-pleven.com	RSA 2048 bits	Let's Encrypt Authority X3	**A**
student.nbu.bg	RSA 2048 bits	RapidSSL SHA256 CA - G3	**A**
meduniversity-plovdiv.bg	RSA 2048 bits	cPanel, Inc. Certification Authority	**A**
www.unwe.bg	RSA 4096 bits	RapidSSL SHA256 CA - G3	**F**
tu-sofia.bg (не е за www.tu-sofia.bg или за *.tu-sofia.bg)	RSA 1024 bits	Let's Encrypt Authority X3	**A+**
uni-plovdiv.bg	RSA 2048 bits	GlobalSign Organization Validation CA - SHA256 - G2	**F**
www.ue-varna.bg	RSA 2048 bits	Let's Encrypt Authority X3	**B**
www.swu.bg	RSA 4096 bits	COMODO RSA Domain Validation Secure Server CA	**F**
www.uni-vt.bg,	Липса поддръжка на протокол за защитена връзка		
www.tugab.bg	RSA 2048 bits	RapidSSL SHA256 CA	**A**
www.tu-varna.bg	Липса поддръжка на протокол за защитена връзка		
mu-sofia.bg	Липса поддръжка на протокол за защитена връзка		
mu-varna.bg	Липса поддръжка на протокол за защитена връзка		
uacg.bg	RSA 2048 bits	Let's Encrypt Authority X3	**F**
mgu.bg	Липса поддръжка на протокол за защитена връзка		
dl.uctm.edu	Липса поддръжка на протокол за защитена връзка		
www.btu.bg	Липса поддръжка на протокол за защитена връзка		
www.vfu.bg	RSA 2048 bits	COMODO RSA Organization Validation Secure Server CA	**C**

Източник: Използван е анализатор за оценка на ssl сертификати https://www.ssllabs.com/ssltest/analyze.html. Оценката е проведена на 9.05.2018

През последните години се наблюдават множество атаки, възползващи се от слабости в системата за имена (DNS) в Интернет. За целта се препоръчва преминаването към защитения протокол DNSSec. DNSSec е предназначен за защита на приложенията от използване на фалшиви или манипулирани DNS данни. Всички отговори от DNSSec защитените зони са цифрово подписани. Чрез проверка на подписа може да се провери дали информацията е идентична (т.е. немодифицирана и пълна) с информацията, публикувана от собственика на зоната. От 2007 г. фирма „Регистър.БГ“, обслужващият имената в област .bg регистратор, предоставя на потребителите си интерфейс за работа с DNSSEC, чрез който всеки регистрант на домейни в зоната .bg и подзоните може да управлява и конфигурира DNSSEC, използвайки сертификат за електронен подпис. За съжаление, само две висши училища в България са подсигурили името си чрез цифров подпис (вж. Таблица 4). По наше мнение е необходимо да се обърне по-голямо внимание и да се приложат добрите практики за внедряване DNSSec (DNSSEC Operational Practices).

Таблица 4
Оценка на защита на домейн имената на ВУ в България

Зона	Наличие на DNSSec
aubg.edu	No DNSKEY records found
uni-ruse.bg	No DNSKEY records found
uni-sofia.bg	Found 2 DS records for uni-sofia.bg in the bg zone Found 1 RRSIGs over DS RRset RRSIG=40422 and DNSKEY=40422 verifies the DS RRset Found 3 DNSKEY records for uni-sofia.bg DS=43438/SHA-256 verifies DNSKEY=43438/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=26106 and DNSKEY=26106 verifies the DNSKEY RRset

	www.uni-sofia.bg A RR has value 62.44.96.22 Found 1 RRSIGs over A RRset RRSIG=26106 and DNSKEY=26106 verifies the A RRset
unibit.bg	No DNSKEY records found
uni-svishtov.bg	Found 1 DS records for uni-svishtov.bg in the bg zone DS=39667/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=40422 and DNSKEY=40422 verifies the DS RRset Found 2 DNSKEY records for uni-svishtov.bg DS=39667/SHA-256 verifies DNSKEY=39667/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=39667 and DNSKEY=39667/SEP verifies the DNSKEY RRset
vtu.bg	No DNSKEY records found
uni-pleven.com	No DNSKEY records found
nbu.bg	No DNSKEY records found
meduniversity-plovdiv.bg	No DNSKEY records found
unwe.bg	No DNSKEY records found
priem.tu-sofia.bg	No DNSKEY records found
uni-plovdiv.bg	No DNSKEY records found
ksp.ue-varna.bg	No DNSKEY records found
swu.bg	No DNSKEY records found
uni-vt.bg,	No DNSKEY records found
tugab.bg	No DNSKEY records found
tu-varna.bg	No DNSKEY records found
mu-sofia.bg	No DNSKEY records found
mu-varna.bg	No DNSKEY records found
uacg.bg	No DNSKEY records found
mgu.bg	No DNSKEY records found
uctm.edu	No DNSKEY records found
www.btu.bg	No DNSKEY records found
vfu.bg	No DNSKEY records found

Източник: Използван е анализатор за оценка на DNSSecc сертификати http://dnssec-debugger.verisignlabs.com. Оценката е проведена на 9.06.2018

Заключение

Висшето училище е специфична законово регламентирана институция, която развива информационната си сигурност във високорискова среда на обмен на информационни записи, фокусирани както върху значителен набор от обучаеми студенти и научни работници от една страна, така и върху уникални процеси, документи и инструкции, осигуряващи триединството на съобразени със стандарти за качество дейности – обучение, научни изследвания, администрация. Информационната сигурност във висшето училище е проблем с нарастваща важност в модерното общество.

През последните години се отбелязва промяна в типа и интензитета на атаките към комуникационната инфраструктура на едно висше училище. Проведеният анализ за оценяване на прилагането на добрите практики показва, че голяма част от висшите училища не отделят сериозно внимание на осигуряване на защитата на комуникациите, поради което не може да се осигури надеждна и сигурна връзка към Интернет.

След направените анализи, бихме препоръчали следните основни мероприятия, които да повишат сигурността на Интернет комуникациите във висшите училища в България:

- използване на повече от един доставчик на Интернет и динамична маршрутизация;
- придобиване на собствено Интернет адресно пространство;
- използване на протокол IPv6;

- използване на конфигуриран съобразно с добрите практики протокол HTPPS;
- защита на името на Интернет областта чрез протокол DNSSec.

Решаването на проблемите свързани с информационната сигурност в едно висше училище не трябва да бъде кампанийно или да води до ограничаване на възможностите за обучение и научни изследвания. Трябва да се избере балансиран и проектно ориентиран подход за изграждане на цялостна архитектура на системата за информационна сигурност.

Използвана литература

'Malware-as-a-service' Market Booms as Prices for Malware and Botnet Creation Tools Decline. (н.д.). Изтеглено на 22 март 2017 г. от Enigma Software: http://www.enigmasoftware.com/malware-service-market-booms-prices-malware-botnet-tools-decline/

Alleged hacker charged with stealing over four million documents from MIT network. (19 юли 2011 г.). Изтеглено на 22 март 2017 г. от U.S. Department of Justice: https://www.justice.gov/archive/usao/ma/news/2011/July/SwartzAaronPR.html

Botcoin: Bitcoin Mining by Botnet. (н.д.). Изтеглено на 22 март 2017 г. от Krebs on Security: http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/

Calvert , S. (3 март 2014 г.). Hacking incidents prompt universities to rethink balance between openness, security. *Baltimor Sun*. Извлечено от http://www.baltimoresun.com/news/maryland/bs-md-higher-ed-hacking-20140315-story.html

Chronology of Data Breaches. (н.д.). Изтеглено на 22 март 2017 г. от Data Breach: https://www.privacyrights.org/data-breach

SSL and TLS Deployment Best Practices. (8 юни 2016 г.). Изтеглено на 22 март 2017 г. от https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

Скандал с Мис България - отнеха титлата на Ина Манчева. (н.д.). Изтеглено на 3 март 2017 г. от 24 Часа: https://www.24chasa.bg/Article/1355332