Изследване на поддръжката на https в електронните магазини на малките и средни предприятия в българия

ас. Ангелин Лазаров Лалев, a.lalev@uni-svishtov.bg
Катедра „Бизнес информатика“,
СА „Д. А. Ценов“- Свищов

Резюме: Настоящата статия представя резултатите от практическо изследване, проведено двукратно (през месец май 2016 г. и отново - през месец януари 2017 г.) с помощта на автоматизирани инструменти за тестване на пробиви. Изследването обхваща една и съща съвкупност от 480 електронни магазина, собственост на малки и средни предприятия в България. То има за цел да установи до каква степен тези предприятия успяват да внедрят правилно HTTPS протокола при защита на електронните си магазини. Изследването е проведено двукратно в опит да се получи информация как и доколко малките и средни предприятия в България успяват да реагират на рязкото повишаване на изискванията към информационната сигурност на Интернет в последните две-три години.

Ключови думи: HTTPS, електронни магазини, инструменти за тестване на пробиви, криптография

JEL: C88, C89

Survey Of The Support For Https In The Electronic Stores Of Bulgarian Small And Middle-Sized Enterprises

Assist. Prof. Angelin Lalev, a.lalev@uni-svishtov.bg
Department of Business Informatics,
D. A. Tsenov Academy of Economics - Svishtov

Abstract: This article presents an empirical survey, conducted in May 2016 and again in January 2017 with the help of software for automated penetration testing. The survey encompasses fixed set of 480 electronic stores, belonging to small and middle-sized enterprises in Bulgaria. The goal of the survey is to determine to what extent such enterprises manage to deploy HTTPS correctly in defense of their electronic transactions. The survey is conducted twice in a 6 month period with aim to obtain information how and to what extent the small and medium-sized enterprises in Bulgaria are adapting to the sharply rising requirements for information security in Internet.

Keywords: HTTPS, electronic stores, penetration testing, cryptography

JEL: C88, C89

Въведение

С все по-широкото навлизане на Интернет продължава да нараства и броят на малките и средни предприятия (МСП) в България, които откриват свои електронни магазини и се ориентират към онлайн продажби. В хода на този процес МСП се сблъскват с различни технологични предизвикателства, свързани с информационните и комуникационните технологии.

Особено важно предизвикателство, което рефлектира не само върху конкурентоспособността на МСП, но и върху потребителските и лични права на клиентите, е осигуряването на информационната сигурност на електронните магазини. Пазаруването онлайн в никакъв случай не би трябвало да води до разкриване финансовото състояние, потребителските предпочитания, личните данни или идентификаторите и ключовете за достъп на потребителя пред трети неоторизирани страни, които евентуално биха се опитали да получат нелегитимен достъп до подобни данни.

За съжаление, развитието на информационните технологии не само подобри средствата за електронна търговия и електронни разплащания, но предостави и солиден арсенал от средства за провеждане на атаки срещу информационната сигурност. Тези атаки днес се извършват в безпрецедентни мащаби и се характеризират с ненадминатата до момента техническа изтънченост.

Противодействието на подобни атаки е свързано с разходи и достъп до релевантното ноу-хау, което при МСП по-често от средното води до това, че проблемът не бива адресиран адекватно. Все по-често МСП се оказват обект на атаки срещу информационната сигурност, независимо от по-малката възвращаемост на вложените усилия от страна на атакуващите. Това ново явление се изучава активно, като отговорните власти в повечето от най-развитите икономически страни вече планират контрамерки[1].

Засега в България на този проблем се отдава по-малко значение поради редица причини, свързани с факта, че електронните разплащания засега изостават, а на защитата на личните и потребителските права онлайн все още се гледа много по-несериозно отколкото в други държави от ЕС, където редица адвокатски групи са много активни при правното представяне на засегнатите потребители и налагането на глоби на предприятията, които са изложили личните им данни на риск. Това обаче неминуемо ще се промени, тъй като рано или късно същите технологични и правни трансформации ще станат факт и в България. Възможно е това да се случи изненадващо бързо и да създаде ситуация, при която внедряването на адекватни контрамерки не може да се осъществи достатъчно бързо от страна на МСП поради чисто логистични пречки, които винаги изобилстват при промяна на информационната инфраструктура.

Настоящата статия представя изследване, което има за цел да разкрие доколко МСП в България се справят с усвояването на основен и сравнително лесен за прилагане компонент на информационната сигурност – прилагането на HTTPS протокола. Изследването е проведено два пъти в рамките на 8 месеца върху една и съща съвкупност от 480 електронни магазина на МСП в България в опит да се улови не само моментното състояние, но и динамиката на този процес.

---

1 Вж. напр. (Critical Infrastructure Cyber Community (C3) Program), (US Small Business Administration - Cybersecurity for Small Business)

1. Значение на HTTPS за електронните магазини на малките и средни предприятия в България

HTTPS протоколът е основното средство за реализиране на сигурна комуникация между потребителските браузъри и уеб сървърите в Интернет и като такова той служи за подсигуряване на широк кръг икономически дейности онлайн, включително осъществяването на електронни покупки и разплащания. HTTPS се базира на криптографски техники, които не само гарантират неприкосновеност на предаваната информация, но и позволяват удостоверяването на самоличността на сървъра чрез използването на технологии за електронен подпис.

В последните няколко години и особено от средата на 2013 година насам, употребата на HTTPS търпи съществена трансформация. До приложението на HTTPS се смяташе за оправдано само при подсигуряване на най-критичните елементи на информационната инфраструктура. Това бе така, тъй като внедряването на HTTPS е свързано с разходи и изисква сравнително повече знания и умения от страна на персонала, натоварен с поддръжката на уеб-сървърите.

Развитието на заплахите за информационната сигурност и особено разкритията от 2013 година (Greenwald, 2013) за пробивите в сигурността дори на големите облачни доставчици като Google, Facebook и пр. – не само възродиха дискусията по стари правни въпроси, свързани с неприкосновеността на кореспонденцията в електронното пространство, но и провокираха отговор от страна на основните технологични компании и общности в света. Част от този отговор е стремежът да се наложи употребата на HTTPS протокола за по широк кръг от сайтове с перспективата един ден той да обхване целия уеб.

Като част от мерките за налагане на HTTPS, през 2014 година търсещата машина на Google започна да поставя по-назад във връщаните резултати сайтовете, които не използват HTTPS. Предстоят да влязат в сила още множество мерки с потенциал да навредят на електронните продажби на предприятия, които не се съобразят с тях. Измежду тях изпъква намерението на Google да модифицира най-популярния уеб браузър в света – Google Chrome – така, че той да започне да извежда предупреждения, за всички сайтове, достъпвани през HTTP. Тези предупреждения ще уведомяват потребителите, че достъпът до подобни сайтове е несигурен. Предвижданите промени ще станат активни с внедряването на версия 57 на браузъра в масова употреба, което се очаква да се случи до края на 2017 година. Много е вероятно останалите популярни браузъри като Firefox (разработван от международна общност от независими разработчици), Edge (Microsoft) и Safari (Apple), да последват тази практика в своите нови версии.

Освен мерките, предприети от техническите лидери в света, съществува и теоретичната възможност HTTPS да залегне в регулациите и препоръките на ЕС за повишаване на информационната сигурност в обхвата на съюза.

Дори ако се абстрахираме от заплахите за информационната сигурност и евентуалните правни последици (глоби и обезщетения), които биха имали пробивите в сигурността, мерките за налагане на HTTPS без съмнение ще се отразят върху електронните магазини на малките и средни предприятия в България, които или трябва да внедрят HTTPS или трябва да се примирят с

евентуалните загуби причинени от по-лошото позициониране в търсещите машини и основните браузъри. Ето защо внедряването на HTTPS трябва да се възприема като сериозен въпрос, който би следвало да бъде приоритетен не само за МСП, но и за всички организации.

2. Методология на изследването и формиране на извадката

Извършеното изследване обхваща извадка от 480 електронни магазина на малки и средни фирми в България, за които може да се предположи, че съставляват между 5 и 20% от магазините, притежавани от малки и средни предприятия (Национален статистически институт, 2015a).

За формирането на извадката е използван Google. За целта е съставен списък от 100 основни думи, описващи основните стоки и услуги, предлагани онлайн, като основната част от тези думи са съобразени приблизително с профила на електронните магазини на МСП[2]. След формирането на извадката, с помощта на компютърна програма са генерирани всички комбинации от фразата „електронен магазин“ и дума от списъка. Резултатните фрази са изпратени като заявки към търсещата машина, като най-релевантните 40 резултата са запазени в първоначалния списък от сайтове, който освен имената съдържа и позицията, дадена от Google в заявката. Полученият първоначален списък съдържа значителен брой сайтове, които не са електронни магазини, множество магазини, които не са базирани в България, но поддържат български език за потребителския интерфейс, както и множество повтарящи се сайтове. Поради това от първоначалния списък са подбрани ръчно 480 магазина[3] с най-високи позиции в съответните си заявки, като е отделено внимание в списъка да не попаднат електронни магазини, за които съществуват съмнения, че принадлежат на големи предприятия или франчайз вериги[4]. При ръчното филтриране също така бяха премахнати и определен брой сайтове, които макар и самоопределящи се като електронни магазини, нямат интерактивен характер, т.е. не взаимодействат с потребителя по никакъв начин[5]. Полученият списък с магазини е тестван с инструмента за тестване на пробиви SSLSCAN[6].

Получената извадка едва ли е идеална в статистическо отношение, тъй като всъщност най-релевантните според Google магазини са обикновено тези магазини, които реализират най-много посещения и продажби. Може да се предположи, че фирмите-собственици на тези магазини развиват успешен бизнес и разполагат с

---

2 Известна информация за онлайн продажбите в България може да бъде извлечена от статистиката на НСИ. Вж. (Национален статистически институт, 2015b)

3 Списъкът на тестваните електронни магазини и особено резултатите от изпълнението на SSLScan (xml документ) могат на теория да се използват за провеждане на атаки срещу информационната сигурност на електронните магазини, поради което могат да бъдат предоставени след аргументирано запитване на адреса на автора – a.lalev@uni-svishtov.bg.

44 Например www.emag.bg, www.office1.bg, www.auto1.bg и пр.

5 Така например, подобни сайтове не разполагат с елементи като потребителска кошница, потребителски регистрации и вход и т.н. Тези сайтове основно приемат поръчки по телефона или по други начини, което ги изключва от по-тясното тълкуване на понятието „електронен магазин“.

6 Вж. **https://github.com/rbsec/sslscan**

най-много средства, които да бъдат отделени за защита на информацията. Също така, тъй като Google вече придвижва сайтовете с HTTPS на по-предни позиции в резултатите от търсенията, може да се предположи, че в извадката ще попаднат повече от средния брой сайтове, поддържащи HTTPS.

По същия начин не могат да бъдат дадени абсолютни гаранции, че някой от подбраните магазини в извадката не принадлежи всъщност на голяма фирма или франчайз верига, макар че поради малкия брой такива предприятия в България и тяхната широка известност с голяма степен на сигурност може да се твърди, че подобни изключения ще имат единичен характер.

Всички тези фактори обаче би следвало да действат в една посока, „изместваики“ резултатите в посока по-добро представяне на добрите практики, свързани с HTTPS. В този смисъл получените от извадката резултати могат да се интерпретират като приблизителни горни и долни граници съответно на добрите практики и установените слабости в сигурността на МСП.

Важен въпрос, свързан с формирането на извадката, е даването на оценка за стохастичната грешка при формиране на извадката. Това е важно от гледна точка на възможността поради нея споменатите долни и горни граници да попаднат съответно още по-ниско или по-високо от стойностите в реалната съвкупност.

Измерените в изследването параметри без изключение имат дискретен характер с две възможни стойности. Тези стойности представляват съответно наличието или липсата на определена слабост или контрамярка. Формирането на извадката от своя страна изключва повторението на магазини. Особеният момент, който трябва да бъде отчетен, са съмненията, че размерът на извадката може да надминава значително 10% от броя на всички електронни магазини в България. Съществуват статистически данни на НСИ за броя на предприятията с над 10 човека, които през 2015 са продали стоки или услуги чрез Интернет (Национален статистически институт, 2015а). Според нея, броят на електронните магазини възлиза на около 2400.

При това положение, тъй като отделните магазини не се повтарят в извадката, най-консервативният подход би бил грешката да не бъде оценявана на база нормално приближение на биномно разпределение, тъй като това може да доведе до нейното подценяване. Вместо това могат да се използват следната горна и долна граници, които са по-консервативни и предполагат моделирането на извадката чрез хипергеометрично разпределение (Chvatal, 1979):

$$P\left(k < \left(\frac{K}{N}\right)n - tn\right) < e^{-2t^2n}$$

$$P\left(k < \left(\frac{K}{N}\right)n + tn\right) < e^{-2t^2n}$$

където k е броят на елементите с наблюдаваното свойство в извадка с размер n елемента, получена от съвкупност с N елемента, К от които с наблюдаването свойство. Т.е. K/N е делът на елементите в истинската съвкупност, а t е параметърът, който показва с колко делът в извадката (k/n) се разминава от реалния в цялата съвкупност.

Тези граници водят до заключението, че **при 480 елемента в извадката, стохастичната грешка възлиза на по-малко 6.2% в 95% от случаите. Тази**

оценка при всички случаи е по-консервативна от тази, която би била получена по пътя на моделирането на извадката като опити със заместване.

3. Резултати от изследването

Първият важен въпрос, на който практическото изследване трябва да отговори, е свързан с дела на подсигурените чрез HTTPS облачно базирани магазини. В това отношение, данните от първото изследване (май 2016 г.) показват интересни факти. Цялостният брой на сайтовете в извадката, които поддържат TLS/SSL и имат валидно Subject поле на X.509 сертификата си (т.е. такова, което отговаря на FQDN името или домейн частта от адреса на сайта), е 139 (28.96%). **Огромният брой на сайтовете, които нямат HTTPS версия е сериозно доказателство за липсата на интерес и ноу-хау относно подходящата защита на информацията в малките и средни фирми.**

Тези 139 сайта могат да бъдат редуцирани по-нататък, като от тях се премахнат SSL сертификати с изтекъл срок (17 броя), както и такива, които са „самоподписани“ (20 броя)**. При редуциране на тези две бройки остават 107 (22.21%) сайта с валиден и проверяем SSL сертификат** /част от сайтовете, които имат самоподписан сертификат също така имат изтекъл срок на сертификата/. За тези сайтове може да се направи допускането, че техните администратори и собственици са сериозно ангажирани с поддържането на сигурен достъп на своите клиенти и служители до магазина. **Ние ще наричаме тази съвкупност „редуцирана“ по-нататък в изложението.**

Повечето от разгледаните в изследването параметри оттук нататък имат смисъл само в контекста на редуцираната съвкупност, тъй като е ясно, че ако даден сайт няма HTTPS сайт с валиден сертификат, повечето изтънчени атаки могат да се заменят с много по-прости и лесни за изпълнение атаки, разчитащи на липсата на HTTPS защита.

Изследването от януари 2017 г. показва подобни резултати. Редуцираната съвкупност при него възлиза на 110 сайта с валиден и проверяем SSL сертификат, което в никакъв случай не представлява съществен прогрес.

Таблица 1
Сайтове с валидни SSL/TLS сертификати

	Изследвани ел. магазини	**Валидни, подписани от сертификационна власт сертификати с неизтекъл срок на валидност**
май 2016	480	107
януари 2017	480	110

Интересно наблюдение може да бъде направено на база Subject полето на невалидните X.509 сертификати. Оказва се, че много облачни доставчици на електронни магазини под модела на „софтуер като услуга“ (SaaS) винаги създават HTTPS версия на сайта, дори такава да не се поддържа от електронния магазин.

Тази HTTPS версия е разпознаваема по невалидния сертификат и съдържанието на полето "Subject". Така например, най-големият доставчик на SaaS електронни магазини в България поставя текста „you.are.not.supposed.to.be.here" в това поле. 106 от общо 389 получени сертификата в повторното изследване имат тази стойност, като поне още 20 имат разпознаваеми Subject полета, които водят към разпознаваем SaaS доставчик. По този начин може да се направи приблизително заключение колко електронни магазина в извадката са изградени на база SaaS усулга, в противовес на другите подходи, които предполагат закупуване на собствени сървъри и широколентов достъп до Интернет, както и на закупуването на PaaS и IaaS сървъри от доставчик на подобни облачни услуги.

Това наблюдение на свой ред води до още един важен за информационната сигурност извод. Тъй като SaaS-базираните електронни магазини прехвърлят цялата работа по специализираната конфигурация към персонала на облачния доставчик и разтоварват МСП от нуждата за извършват подобни специфични дейности, фактът че голямо множество от SaaS-базираните магазини не използват HTTPS подсказва, че причините за слабата поддръжка на HTTPS трябва да се търсят или в размера на разходите (100 до 500 USD годишно за SSL сертификат) или в абсолютната неинформираност на МСП с мерките и технологиите на защита в Интернет.

Редуцираната съвкупност на свой ред съдържа интересна информация. В проведеното през месец май 2016 г. проучване, 4 сайта от редуцираната съвкупност (3.73%) поддържат gzip компресия на HTTP хедърите, което ги прави податливи на атаката CRIME[7]. Шест месеца по-късно в редуцираната съвкупност няма податливи сайтове.

Изследването от май 2016 г. също показва, че 38 (35.51%) от цялата и 106 (**99.07%**) от сайтовете в **редуцираната** съвкупност поддържат съответно SSL3.0 и TLS1.0 което ги прави податливи в различна степен на атаката POODLE[8], при условие, че тези сайтове също поддържат набори от шифри, които разчитат на симетричен шифър в CBC режим на работа и при условие, че потребителските браузъри не са специфично конфигурирани за избягване на атаката. Подобна е и ситуацията с изследването от месец януари 2017, при което 101 от 110 сайта в редуцираната съвкупност поддържат SSL3.0 или TLS1.0 в комбинация с DES-CBC шифър. Това означава, че **91.82%** от сайтовете в редуцираната съвкупност са податливи на POODLE при условие, че потребителският браузър поиска при договарянето засегнатите набори от шифри.

---

[7] CRIME ("Compression Ratio Info-leak Made Easy") е атака, която използва компресията на HTTP заглавната част като криптографски оракул (най-общо, устройство или дефект на системата, от който изтича определена информация). На база изтичащата информация атакуващ с възможност да променя трафика може да възстанови бисквитките на сесията и да я „отвлече", влизайки в ролята на потребителя на ел. магазин. CRIME е част от фамилия подобни атаки. Вж. (Prado, Harris, N., & Gluck, Y., 2013).

[8] POODLE ("Padding Oracle on Downgraded Legacy Encryption") е атака, която разчита на слабости в договарянето на SSL/TLS шифри. Атакуващ с възможност да прихваща и подменя трафика може да предизвика ситуация в която дешифрирането на връзката на HTTPS става тривиално и от там той може да чете и променя съдържанието на трафика между клиента и сървъра. Вж. (Moeller & Duong, 2014)

Прави впечатление, че делът на сайтовете, поддържащи SSLv3.0 в редуцираните съвкупности е чувствително по-висок от този на сайтовете в цялата извадка. **Тази разлика може да се обясни само с предположението, че активно работещите магазини целенасочено понижават настройките си за защита, да акомодират остарели портебителски браузъри, характерни за системи като Windows XP и Android 2.x и т.н.**

POODLE е особено ярка илюстрация за много от проблемите, свързани с подсигуряването на HTTPS. Тази атака съществува на първо място поради механизмите за обратна съвместимост, залегнали в HTTPS. Тези механизми позволяват по-стари браузъри и системи да се свързват с по-нови сървъри и обратното. Тъй като HTTPS функционира в разпределена и хетерогенна среда, без тази обратна съвместимост, самото му използване на практика би било много трудно. Най-старите механизми за сигурност обикновено са първите, които стават обект на практически изпълними атаки, което налага много фино балансиране между сигурността на връзката и кръга на системи, които могат да се свързват една с друга. Този баланс е в постоянна динамика, тъй като се влияе от бързо развиващите се криптографски техники и техните контрамерки. Именно това е причината, поради която правилното прилагане на HTTPS изисква нетривиални знания и умения от страна на ИТ персонала, конфигуриращ уеб сървърите. Именно ИТ персонал с такава подготовка е малко вероятно да бъде на разположение на МСП, което прави тяхната задача още по-трудна.

TLS1.0 и особено SSL3.0 са два остарели варианта за реализиране на HTTPS, които обаче се поддържат наред с по-новите за да може да се акомодира достъпът на стари браузъри, които не се обновяват повече. С появата на POODLE стана ясно, че шифър DES в режим на CBC, съчетан с SSL3 или TLS1.0 не е повече сигурен начин за подсигуряване на комуникациите, което наред с едновременните пробиви в RC4 остави само две алтернативи. Първата от тях е на остарелите системи (Windows XP, Android 2.x) да се отказва достъп до сайта въобще. Другата алтернатива е да се позволи несигурен достъп, като при това потребителите няма да бъдат предупредени експлицитно за това от остарелите си браузъри. Изборът на електронните магазини по отношение на подобни потребители, очертан от данните, изглежда логичен и се изразява в изказаната по-горе хипотеза.

Подобна е и ситуацията с комплектите от шифри, базирани на RC4. Въпреки че информацията за техните слабости е известна от началото на 2015 година, изследването от м. март 2016 показва, че 51 електронни магазина от редуцираната съвкупност (47.67%) поддържат набор от шифри, в който RC4 се използва в ролята на симетричен шифър. От тях 35 поддържат RC4 в иначе силни набори от шифри, съставени от Дифи-Хелман обмен върху елиптична крива и SHA256/SHA384.

В изследването от м. януари 2017 г. 31 от 110-те сайта в редуцираната съвкупност (**28.18%**) използват RC4, като в 21 от случаите, RC4 се използва в шифри, които използват силни криптографски механизми в ролята на останалите криптографски примитиви (хеш функции и механизми за perfect forward secrecy на сесията).

Също като при POODLE, за да се експлоатират грешките в RC4, клиентът също трябва да се съгласи на предложения набор от шифри, което може да е при

използването на остарял софтуер или целенасочено понижени настройки за сигурност при клиента.

В редуцираните съвкупности от май 2016 г. и януари 2017 г. има и 2 електронни магазина (съответно 1.87% и 1.82%), които поддържат Дифи-Хелман обмен на база 512 битови групи. Ограничението от 512 бита е следствие от регулацията за ограничаване на износа на криптографски технлогии, действала през 90-те години на миналия век в САЩ. За съжаление, шифрите, които я поддържат (известни като „Export" шифри) не бяха премахнати до скоро от основните библиотеки за реализиране на SSL/TLS. Като резултат, при грешна конфигурация на HTTPS, какъвто е наблюдаваният случай, съответните шифри са податливи на Logjam[9] атаки, които разчитат на напредъка на хардуера и числовите алгоритми за изчисляване на дискретния логаритъм.

Получената информация може да бъде обобщена по следния начин (вж. табл. 2):

Таблица 2
Обобщени данни за открити слабости в реализацията на HTTPS

	CRIME(%)	**POODLE(%)**	**RC4(%)**	**Logjam/Export**
май 2016	3.73%	99.07%	47.67%	1.87%
януари 2017	0%	91.82%	28.18%	1.82%

От таблицата е видно, че тези магазини, които използват HTTPS променят конфигурациите си в посока постигане на сигурност, но този процес е крайно бавен и вероятно е възпрепятстван от необходимостта да се поддържат голям брой остарели браузъри, операционни системи и мобилни устройства, използвани от потребителите в България.

4. Заключение

На база на изложените данни, могат да се направят някои изводи и предложения.

На първо място се налага изводът, че преобладаващата част от магазините на българските малки и средни предприятия не са съобразени не само с новопоявяващите се технически „изтънчени" атаки, но всъщност не прилагат HTTPS въобще.

От множеството на предприятията, които прилагат HTTPS, може да се заключи също, че малките и средни предприятия не са готови на техническо и концептуално ниво за осъществяването на прехода към изцяло електронни разплащания и евентуалните ползи, които биха последвали от разширяване на

[9] Logjam атаките разчитат на понижаването на сложността на проблема за изчисляване на дискретен логаритъм (на който се базира сигурността на Дифи-Хелман обмена) чрез предварително изчисляване на някои фиксирани в по-старите стандарти на SSL/TLS числови групи или чрез деградиране на протокола до 512 битови групи, което е възможно, ако системата поддържа старите „Export" шифри.

дейността в други държави на ЕС. Същото важи и по отношение на евентуалното увеличаване на броя на притежателите на кредитни карти в България.

Важен извод произтича и от наблюдението, че много магазини на МСП вероятно целенасочено понижават настройките си за сигурност. Това може да се обясни само с нуждата да се акомодират по-стари компютърни системи и мобилни устройства, които по необходимост са инсталирани с морално остарял софтуер. В хода на този процес потребителите на тези системи биват изложени на риск за информационната сигурност, тъй като в тази ситуация само сървърът може да предотврати слаби настройки на HTTPS.

Може да се предположи също, че делът на тези остарели устройства ще остане по-висок спрямо най-развитите държави в света, което добавя национална специфика на проблема и естествено възпрепятства процеса на подсигуряване на HTTPS, тъй като сигурността на протокола зависи от най-слабото звено в него, било то електронния магазин или потребителя.

Поради тясната връзка на HTTPS с електронните разплащания, получените данни могат да се тълкуват в паралел с факта, че за момента МСП в България прилагат различен подход към заплащането на закупени онлайн стоки и услуги. При електронното пазаруване в България често се използва наложен платеж, който е задоволителен механизъм и алтернатива на електронните плащания. Той обаче има много недостатъци спрямо разплащането с кредитни и дебитни карти. Освен необходимостта плащанията да се осъществяват с налични в брой средства и невъзможността да се продава на клиенти в чужбина, наложният платеж крие друг латентен, но сериозен риск за МСП. Тъй като наложният платеж има по-малко възможности за проследяване на плащанията, той може да бъде регулиран или дори забранен в бъдеще, което ще остави плащанията с дебитни и кредитни карти единствената друга алтернатива и ще принуди МСП да извършат бързи внедрявания, често за сметка на сигурността на клиентите.

По отношение на сигурността на самите потребители и на това как МСП виждат своите ангажименти в тази посока, също могат да се направят важни заключения. Данните водят до извода, че при наличие на избор дали достъпът на потребител до сайта да бъде забранен или вместо това той да бъде осъществен при (понякога драстично) намалено ниво на сигурност без потребителят да бъде специфично уведомен, МСП биха избрали първия вариант. Усилията на Google и други технологични компании за налагането на общи стандарти за приложението на HTTPS протокола засега не дават желания ефект в България. Демотирането на сайтовете в резултатите на търсещите машини засега не изглежда да води до особени ефекти върху използването на HTTPS при електронните магазини на МСП в България. Това на свой ред налага заключението, че МСП не са информирани или не възприемат мерките на Google и технологичния сектор като препятствие пред електронните си продажби.

Могат да бъдат направени и някои предложения за мерки, които биха способствали не само за повишаване на сигурността на МСП, но и биха повишили конкурентоспособността на българските търговци онлайн.

В България вече съществува национален център за действие при инциденти в информационната сигурност (CERT.BG). Функциите на този център, обаче, за момента се свеждат до разпращане на информационни бюлетини и докладване на

инциденти. Този център би могъл да разшири своята дейност в посока разработване на информационни материали за повишаване на информационната сигурност на МСП и в частност – на техните електронни магазини.

Националните доставчици на квалифициран електронен подпис не са сертифицирани, което означава, че все още много от тях не могат да издават SSL/TLS сертификати, които се признават от основните браузъри. Ако те бъдат задължени да проведат такава сертификация, издаването на електронни сертификати може да се превърне в национална дейност, което би следвало да смъкне цените за закупуване на електронен сертификат. Това решение носи допълнителни предимства, тъй като много МСП вече използват електронни подписи от същите доставчици и познават процедурата на издаване.

И не на последно място, друга мярка, която трябва да бъде въведена е обновяване на законовата база, касаеща обезщетяване на клиенти, претърпяли щети вследствие на пробиви в информационната сигурност на фирми, обработващи техни данни.

В заключение трябва да се спомене, че колкото и важно, прилагането на HTTPS е само една от нужните технически мерки за подобряване на информационната сигурност, която трябва да се комбинира с мерки за противодействие на всички други заплахи. Сложният комплекс от заплахи и контрамерки ще остава солидно предизвикателство пред МСП в следващите години и ще бъде основна област за експериментиране на нови стратегии и внедряване на подобрени решения.

Използвана литература

Chvatal, V. (1979). The Tail of Hypergeometric Distribution. *Discrete Mathematics, 25*, 285-287.

Critical Infrastructure Cyber Community (C3) Program. (n.d.). Retrieved 03 02, 2017, from https://www.us-cert.gov/ccubedvp

Greenwald, G. (2013, Sep 6). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*.

Moeller, B., & Duong, T. (2014). This POODLE bites: Exploiting the SSL 3.0 fallback. *Google Security Advisory*.

Prado, A., Harris, N., & Gluck, Y. (2013). SSL Gone in 30 seconds - a BREACH beyond CRIME. *BLACKHAT'2013.*

US Small Business Administration - Cybersecurity for Small Business. (n.d.). Изтеглен на 03.02, 2017, from https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

Weak Diffie-Hellman and the Logjam Attack. (n.d.). Изтеглен от https://weakdh.org/

Национален статистически институт. (2015a). *Предприятия, които са получавали поръчки онлайн за 2015*. Изтеглен 2015, от http://www.nsi.bg/bg/content/2872/предприятия-които-са-получавали-поръчки-онлайн-продажби

Национален статистически институт. (2015b). *Вид на поръчваните стоки и услуги от лицата по интернет*. Изтеглен 2015, от http://www.nsi.bg/bg/content/2833/вид-на-поръчваните-стоки-и-услуги-от-лицата-по-интернет.