ЕДИН ПОДХОД ЗА ФОРМИРАНЕ НА ПОЛИТИКА ЗА БЕЗОПАСНОСТ И ЗАЩИТА НА ДАННИТЕ В МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ[1]

доц. д. ик. н. Румен Върбанов
доц. д-р Веселин Попов[2]

Въведение

Последните години сигурността и защитата на данните се превърна в приоритет проблем, от който в много голяма степен зависи нормалното функциониране на бизнес информационните системи. Киберпрестъпността вече е професионално и дори търговско занимание, а нейните методи станаха по-изтънчени и скрити. Анализът на тенденциите в поведението и целите на съвременните интернет престъпници при корпоративните атаки показва наличие на изключително много целенасочени атаки, осъществени чрез кражба на лични данни и злоупотреба с тях. С други думи, ако до момента вирусите се пишеха от аматьори, сега вече те целят финансова изгода и дори се използват за политически и терористични цели.

Когато се говори за безопасност в Интернет става дума за много съществена част на политиката към Интернет, от която до голяма степен зависи успешното използване на Мрежата в бизнеса, обучението, държавното управление и много други области. Тази политика трябва да се формира като се отчита натрупаният опит в света и при задължителното участие на всички заинтересовани страни – бизнес, правителства, гражданско общество и технически експерти.[3] От друга страна рисковете, предизвикани от постоянното развитие на електронния бизнес в световен мащаб, се развиват толкова бързо, че специалистите по информационна безопасност не са в състояние адекватно да реагират на тях и да осигурят надеждно функциониране на информационните системи. Много анализатори споделят мнението, че е необходимо да се разработят съвършено нови методи и технологии за осигуряване безопасността на бизнеса в Web.

Налице са много доказателства за това, че *информационната среда на малките и средни фирми е по-уязвима* към пробиви в сигурността. Въпреки това проблемите на безопасността на малкия и среден бизнес в нашата страна силно се подценяват. Усилията се насочват основно към разработването и функционирането на сайта като се пропускат в стратегията проблемите на безопасността на търговските онлайн процеси. По този начин от самото начало не се отчитат някои основни изисквания за резултатна електронна търговия и това впоследствие се отразява негативно върху начинанията. Причините се коренят в силно ограничените средства за ИКТ и закупуване на съвременно мрежово оборудване и технологии за защита. Традиционно се *омаловажава ролята и значението на ИКТ и безопасността*, тяхното решаване се оставя на

---

[1] Настоящата статия представя част от резултатите по Проект № 9-2010 “Изследване на състоянието на сигурността на данните в бизнес информационните системи на малки и средни предприятия и разработване на политика и стратегия за информационна сигурност”. СА “Д. А. Ценов” – Свищов, 2010 г.

[2] Участието на авторите в настоящата статия е както следва: доц. д. ик. н. Румен Върбанов – въведение, т. 1,т. 2 и заключение; доц. д-р Веселин Попов – т. 3.

[3] An Inventory of Policy Positions and Practical Guidance ICC’s Commission on E-Business, IT and Telecoms (EBITT). First edition 2007. http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/Statements/EBITT%20Inventory%20Brochure.pdf

последно място в приоритетите като в повечето случаи липсва ясна перспектива и дългосрочно стратегия. Омаловажават се щетите, които персоналът може да причини на МСП в качеството си на най-непредвидимата и неконтролируемата уязвимост за сигурността, и не се инвестира в обучение и повишаване на информационната култура на служителите.

1. Подход към създаването на политика за безопасност в малките и средните предприятия

От предишното изложение в тази част стана ясно, че развитието на електронната търговия в национален и международен план в най-голяма степен се определя от прогреса в областта на безопасността на информацията.

Формирането на политика за безопасност на електронната търговия в МСП е наложително, за да се говори до голяма степен за насърчителни резултати от функционирането й. Но това на практика е сложен и труден за решаване проблем поради няколко причини, които може да се представят така:

- ограничените възможности на МСП по отношение на финансови средства, ИТ специалисти и съвременна инфраструктура;
- подценяване на проблемите и опасностите, свързани със сигурността на информацията в МСП;
- бързото развитие на Интернет технологиите;
- непрекъснатият прогрес в създаването на зловредни програми, техният все по-професионален и комплексен характер;
- ниското ниво на подготовка на служителите;
- трудностите, свързани със задаването и спазването на правила за безопасност в предприятието;
- слабо разпространената практика на малкия и среден бизнес в България да използва услугите на ИТ аутсорсинга, вкл. за безопасност на електронната търговия;
- ограничените решения на системите за електронна търговия, които малкият и среден бизнес в България използва понастоящем.

Нашите проучвания показват, че голяма част от МСП, които имат определени амбиции за ефективно присъствие в Web, насочват усилията си основно към разработването и функционирането на сайта като пропускат в своята стратегия проблемите на безопасността на търговските онлайн процеси. По този начин от самото начало не се отчитат някои основни изисквания за резултатна електронна търговия и това впоследствие се отразява негативно върху начинанията.

Има много основания да се твърди, че *информационната среда на малките и средни фирми е по-уязвима* към пробиви в сигурността.

Защо се подценяват проблемите на безопасността на МСП в нашата страна?

Първото обяснение е *малкия бюджет за информационни и комуникационни технологии*, с който разполагат. Силно ограничените средства не позволяват да се закупува съвременно мрежово оборудване и технологии за защита, напр. защитни стени за вътрешните мрежи. Действително става дума за скъпи решения и технологии, а поддръжката и безопасността ще прибавят дори допълнителни разходи.

На второ място може да се изтъкне *омаловажаването на ролята и значението на ИКТ и безопасността*, тяхното решаване ден за ден, без наличие на ясна перспектива и дългосрочно стратегия. Трудно се възприема фактът, че

м**алките и средни фирми трябва да разберат, че за инвестициите в сигурност не може да се мисли най-накрая**. Целесъобразно е те бъдат добре планирани, както финансово, така и технически. Отсъствието на стратегическо планиране реално води до състояние, при което бизнесът винаги ще реагира на най-новите спешни случаи, като губи пари и се опитва да го възстановява, и никога няма да може да се фокусира върху разширяването на бизнеса.

На следващо място може да се посочи, че се наблюдава увеличаване на нарушенията и щетите, които *персоналът на предприятието* може да нанесе. Масовото навлизането на електронни устройства в ежедневието и увеличаващия се брой служители, които използват лаптопи в и извън офисите, разширява обхватността на мрежите и това е свързано с увеличаване на заплахите и рисковете. Неконтролируемото използване на флаш памети и мобилни устройства от служителите също крие много рискове за кражба и злоупотреби с конфиденциална фирмен информация.

И накрая, трябва да се посочи, че *обучението е ключов фактор за подобрена мрежова сигурност.* Става дума за обучение на служителите, мениджърите и собствениците на малки и средни фирми. Днес лесно може да се констатира нарастващия ефект, който добре подготвените служители могат да имат върху сигурността на компанията. В същото време компютърните потребители могат да бъдат смятани за най-непредвидимата и неконтролируемата уязвимост за сигурността. В повечето случаи, липсата на образованост и разбиране за основни принципи и процедури на сигурността са главната причина за пробиви в сигурността, а не действията на зловреден код и други вируси.

Целесъобразно е от самото начало, когато се оформят и материализират вижданията за Интернет бизнеса на предприятието да се документират контурите на системата за безопасност и избрания модел и ограничения. При всички случаи тази рамка е основна част на глобалната система за сигурност на предприятието. Именно такъв подход позволява успоредно с организационните и технологични проблеми да се отчетат и проблемите, свързани с безопасното функциониране.

Има няколко **ключови момента** при разработването на политика за безопасност в малкия и среден бизнес:

- анализ и изясняване на това *какви точно данни* и доколко сериозно трябва да се защитят;
- уточняване на това *кой точно и какви щети* може да нанесе на предприятието в информационен аспект;
- приблизително *изчисляване на рисковете* и набелязване на конкретни мерки за тяхното минимизиране;
- набелязване на *конкретни средства*, методи и технологии, които ще се използват за осигуряване безопасността на електронната търговия;
- тестване, реализиране и поддръжка на системата за безопасност

Анализът на натрупания опит ни навежда на мисълта, че в основата на подхода към реализирането на системата за електронна търговия, трябва де се поставят няколко **принципни положения**, които регламентират последващото изработване и спазване на политиката и стратегията за безопасност на данните в предприятието.[4]

[4] Вж. по-подробно: Върбанов, Р. Корпоративни мрежови архитектури и технологии., Академично издателство "Ценов", 2008 г., с. 334 - 354; Върбанов, Р. Компютърни мрежи.,

- идентификация и автентификация;
- съхраняване на данните;
- обработка на поръчките;
- постепенност и етапност;
- използване на водещи технологии и доказани решения, на базата на продукти от фирми лидери в разглежданата област;
- защита на инвестициите;
- защита на транзакциите.

Идентификация и автентификация. Обикновено за всяко приложение на онлайн търговията се използва конкретен метод за идентифициране на потребители и техните права за достъп. Теорията и практиката предлагат множество различни методи и технологии. Изборът на най-подходящите трябва да стане в съответствие с избраният модел за електронна търговия и вижданията на ръководството за неговото развитие в близките 1-2 години.

Съхраняване на данните. Има се предвид мястото за съхраняване на най-съществената част от информацията за функционирането на електронния магазин – каталози, ценови листи, кредитни карти и др. Има различни варианти – съхраняване зад защитната стена или в защитена система. Ясно трябва да се отговори на въпроса как ще се осъществи достъпът до тази информация и дали се предвижда използване на защитени канали.

Обработка на поръчките. Тук се включва комплекс от проблеми, които имат голяма значение за архитектурата на Web сървъра. Най-важните от тях са свързани с това къде ще се обработват онлайн поръчките (на Web сървъра, върху отделен сървър), къде ще се обработват разплащанията с кредитни и дебитни карти, ще се използват ли виртуални частни мрежи и други технологии.

Постепенност и етапност. Спазването на този принцип изисква да се започва с не много скъпа, но достатъчно надеждна архитектура на системата за защита, която да осигури определено ниво на сигурност за конкретната организация. Необходимо е да се отчита, че колкото по-мащабна и сложна става информационната система на предприятието, толкова повече пробиви и уязвимости могат да се инкасират във всеки неин компонент. Затова изискванията за информационна безопасност трябва да се отнасят до всички компоненти на информационната среда на компанията. Впоследствие може да се надгражда и да се ъпгрейдват основните компоненти в зависимост от задачите, които си поставя предприятието при пренасяне на своя бизнес в Интернет.

Използване на **водещи технологии и доказани решения**, на базата на продукти от фирми лидери в разглежданата област. Добре е от самото начало в проекта за електронен бизнес да се предвиди използването на най-съвременните технологии за безопасност с възможности за регулярно обновяване.

Защита на инвестициите. Това означава, че при преминаване към по-сложни и сигурни системи за защита, направените инвестиции в техника и програмно осигуряване трябва да се запазят чрез интегриране на съществуващото оборудване в новите решения, като се прегрупират наличните

Свищов, Академично издателство "Ценов", 2006 г., с. 263-291; Иванов, В. Електронната търговия – заплахи пред информационната сигурност. Трети дискусионен форум "Информационна сигурност", 15 юни 2004.; Иллюстрированный самоучитель по разработке безопасности. http://www.svit-it.com.ua/kb/ds/menu.html; "Методы и средства защиты информации" (курс лекций). http://www.citforum.ru/internet/infsecure/index.shtml; Паргов, Д. Аспекти на информационната сигурност в Интернет. Networkworld България, 2000, бр. 3.

устройства или чрез ъпгрейд се създаде ново качество.

Защита на предаването на данни и транзакции. Тук има два важни момента - защитата на Web сървъра чрез протокола SSL и защитата на клиентския компютър в процеса на взаимодействие, вкл. с възможности за използване на цифрови сертификати.[5] За малкия и среден бизнес обикновено защитата на транзакциите се поема от външната организация, която поддържа сайта. А задълженията и правата на страните се гарантират с SLA (Service Level Agreement, Споразумението за нивото на услугата). За отстраняване на отказите предприятието се обръща към предвидените в SLA функции. Съответните методи трябва да бъдат описани и оптимизирани за всеки конкретен потребител. При определени условия това позволява даже икономия на механизми за резервно копиране и резервиране. Например, за филиал с регулярен трафик от клиенти е важно той да ползва услугата в работно време, а в празничните дни това не е нужно.

2. Съдържание на методиката за създаване на политика за безопасност и защита на данните в малки и средни предприятия

Предлаганата методика за разработване на политика за безопасност на електронната търговия в МСП отчита гореизложените принципни положения и съвременните решения, които днес се използват.[6]

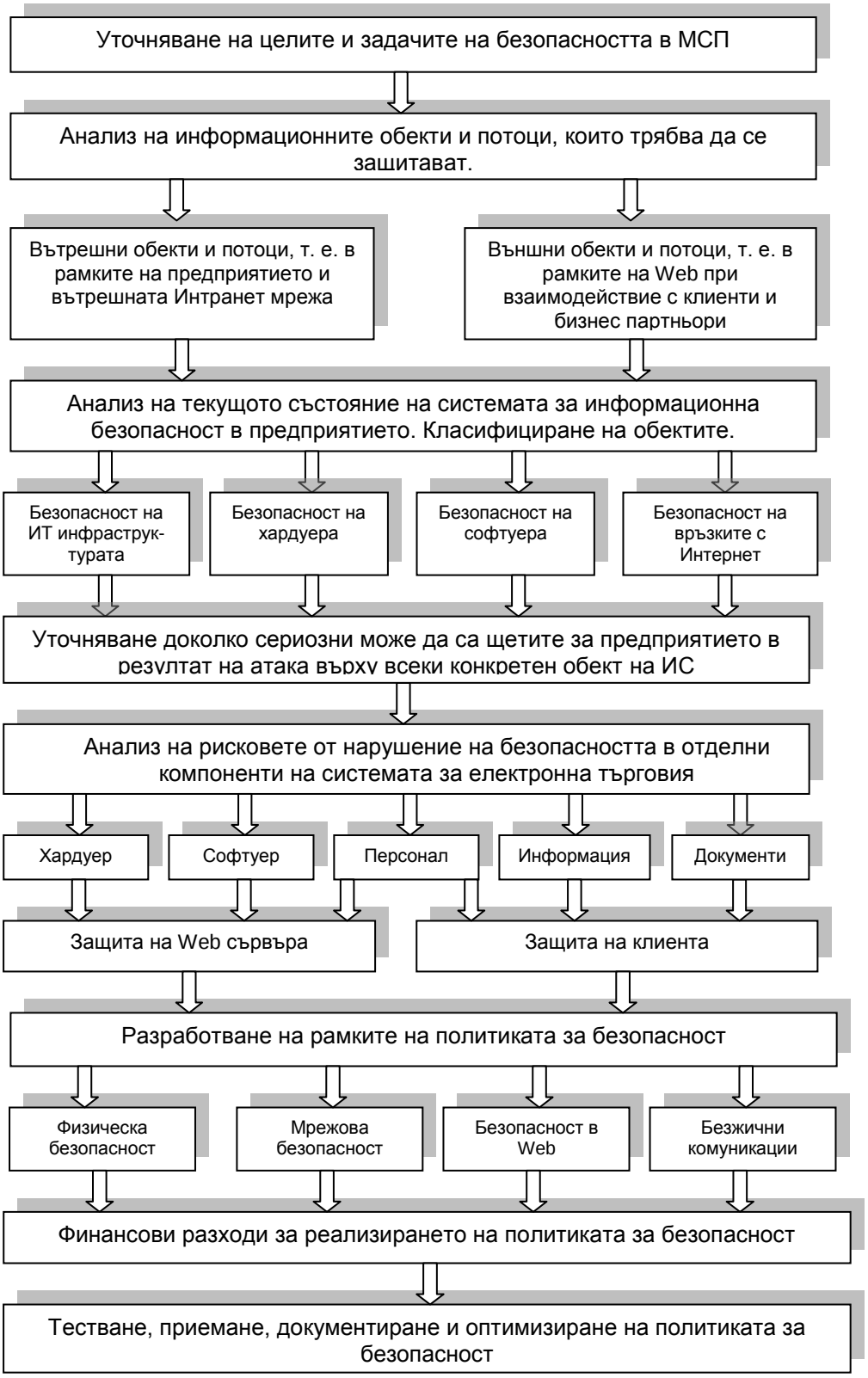
Подходът към разработването на методиката отчита също така резултатите от практическите проучвания на автора относно състоянието на информационната безопасност в българските МСП.

Съдържанието на методиката е структурирано в няколко основни фази, които представят сърцевината на проблемите, свързани със безопасността на данните при електронната търговия (вж. фиг. 1):

- уточняване на целите и задачите на безопасността в МСП. Оценка на рискове и предизвикателствата в Web;
- анализ на информационните обекти и потоци, които трябва да се защитават;
- анализ на текущото състояние на системата за информационна безопасност в предприятието и класифициране на обектите в няколко големи групи;
- уточняване доколко сериозни може да са щетите за предприятието в резултат на атака върху всеки конкретен обект на информационната система;
- анализ на рисковете от нарушение на безопасността в отделни компоненти на системата за електронна търговия;
- разработване на рамките на политиката за безопасност;
- финансови разходи за реализирането на политиката за безопасност;
- тестване, приемане, документиране и оптимизиране на политиката за безопасност.

[5] Вж. Амор, Д. (Р) ЕВОЛЮЦИЯТА на е-бизнеса. Как да живеем и работим в свързания свят. Инфо Дар, С., 2000, с. 497-588; Върбанов, Р. Основи на електронния бизнес. Свищов, Академично издателство "Ценов", 2007 г., с. 301-316.

[6]



Фиг. 1. Методика за създаване на политика за безопасност на електронната търговия в малки и средни предприятия

Ще разгледаме кратко съдържанието на всяка една от основните фази, през които преминава разработването на политиката за безопасност в МСП.

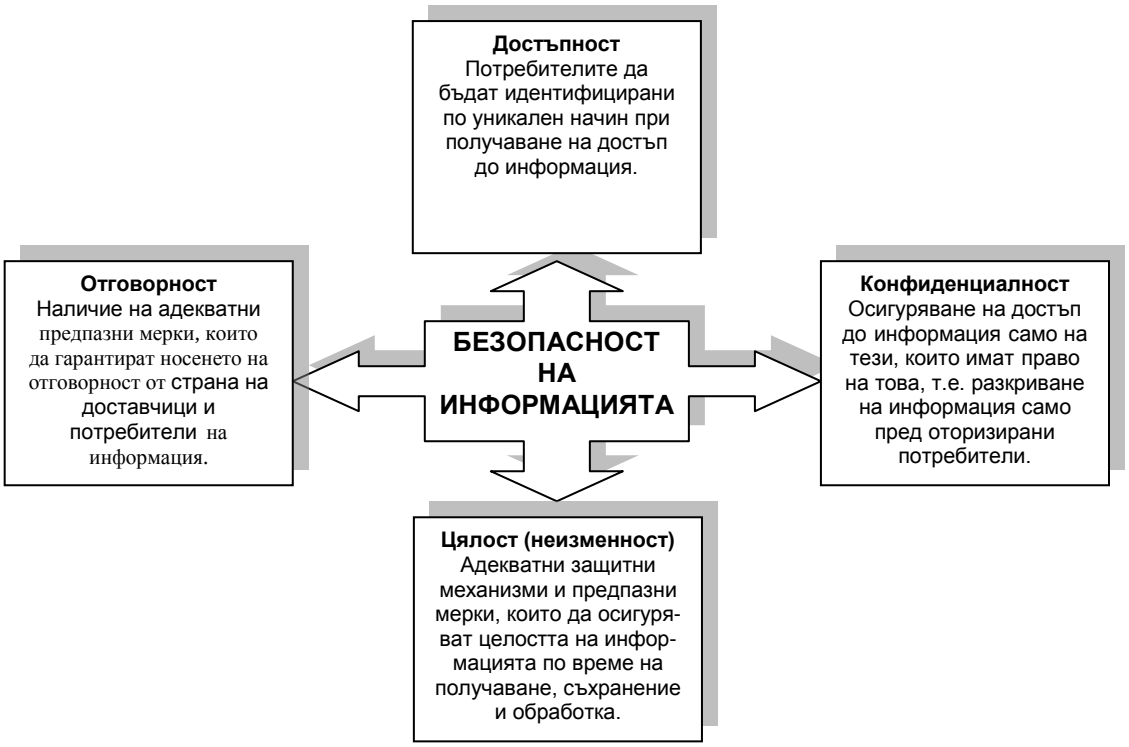
1.1. Уточняване на целите и задачите на политиката за безопасност на електронната търговия

При разработването на политика и стратегия за безопасност на МСП първо трябва да се уточни съдържанието на понятието *безопасност*. Може да се приеме, че това е състояние на устойчивост на информацията към случайни или преднамерени въздействия, изключващо евентуални рискове, свързани с унищожаването на данни, тяхното разкриване или фалшифициране, което може да доведе до материални щети за собственика или притежателят на информация. Горното определение в максимална степен отчита основното предназначение на всяка търговска информация в информационната система на предприятието – изключване на финансови загуби, получаване на печалба от собственика и потребителите на информация в условията на реални рискове. Освен това така формулираната политика за безопасност задава рамка на система от мерки, която е насочена към: - осигуряване на достъпност на информацията (чрез осигуряване на надежден и навременен достъп до информацията); гарантиране на поверителност на информацията (прилагане на система от одобрени правила за работа с информация); осигуряване на цялостност на информацията; постигане на отчетност на информацията (чрез въвеждане на контрол върху достъпа и правата върху информационните системи).

Според нас политиката за безопасност на една малка и средна фирма преследва няколко **цели** – а) осигуряване на непрекъснат процес на работа на предприятието и фокусиране повече върху разрастването на бизнеса, а не върху възстановяването след пробиви; б) минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на конкретното предприятие, неговите клиенти и бизнес партньори; в) идентифициране на основните параметри на политиката за управление на информационната сигурност; г) минимизиране на степента на загуби или вреди, причинени от пробиви в сигурността.

Постигането на горните цели и гарантиране безопасност на информацията изисква решаването на 4 **основни задачи** – осигуряване на нейната достъпност, конфиденциалност, цялостност и отговорност (вж. фиг. 2). И съответно всяка заплаха трябва да се разглежда от гледна точка на това как може да засегне тези четири качества на безопасната информация.[7]

[7] Вж. по-подробно: Върбанов, Р. Корпоративни мрежови архитектури и технологии., Издателство "Faber", 2009 г., 211 с.



Фиг. 2. Постигането на безопасност на информацията изисква решаването на четири основни задачи

Ведомствената политика за сигурност се състои в разработване и утвърждаване на общи и частни **правила и процедури** за сигурност на отделните потребители, отдели и/или дирекции, както и на правила и механизми на взаимодействието помежду им, като включва:

- определяне на застрашените ресурси и услуги;
- уточняване на потребителите, които имат достъп до ресурсите, които трябва да се обезопасят и установяване на контрол на достъпа;
- правила за локална и отдалечена идентификация и автентификация;
- използване на криптографски методи и устройства за защита на данните и контрол на достъпа;
- защита от вируси;
- изготвяне на ръководство по сигурността;
- обучение и подготовка на потребителите.

Правилата са важна част от политиката за безопасност и освен яснота по отношение на конкретните изисквания, те позволяват осъществяването н ефективен контрол и одит върху системата.

1.2. Анализ на информационните обекти и потоци, които трябва да се защитават

Фиг. 3. Процесът на електронна търговия може да се представи в няколко основните фази

Основният въпрос на който трябва да се отговори е *кои са ресурсите, които трябва да се обезопасят*. След това трябва да се идентифицират *потребителите, които имат достъп и използват различните ресурси*.

Анализът на информационните обекти и потоци, които трябва да се защитават се провежда върху всички обекти и информационни потоци, които имат отношение към системата за електронна търговия. При разработването на политика за безопасност трябва да има ясна представа за основните фази. В табл. 1 разгледахме четирите основни етапа, от които е съставен процесът на електронната търговия и заплахите от гледна точка на конфиденциалност, интегритет и достъпност на данните. Тук ще се опитаме да детайлизираме взаимоотношенията между купувача и онлайн търговеца в Интернет. В най-едри щрихи процесът на електронна търговия може да се представи в няколко основните фази (вж. фиг. 3).

Както вече стана ясно на всяка от представените по-горе фази съществуват конкретни рискове и заплахи. Важно е да съществува яснота и

виждане за начина, по който трябва да се противодейства във всяка конкретна ситуация.

1.3. Анализ на текущото състояние на системата за информационна безопасност в предприятието. Класифициране на обектите, които се нуждаят от защита.

Сравнително лесно може да се установи какво е текущото състояние на системата за информационна безопасност в предприятието. За това е необходимо да се познават основните средства и технологии, които се прилагат в малкия и среден бизнес. Нашите проучвания показват, че в МСП се използват основно традиционните средства за защита на данните, като не се познават възможностите на интегрираните решения за осигуряване на безопасността. Силно се подценяват съществуващите рискове с оправданието, че те не се отнасят до малкия и среден бизнес На въпроса „Какви средства и технологии за защита на информацията използвате във Вашето предприятие (възможни са няколко отговора)?" 100% от анкетираните посочват антивирусен софтуер, 47% - антиспам софтуер и само 9% споменават за защитни стени. Очевидно в повечето случаи предприятието от SMB сектора използват най-популярните средства за защита като антивирусни пакети, потребителски имена и пароли и защитни стени. Но няма ясна, системна и целенасочена организация за работа в областта на безопасността на информационната система на предприятието.

На въпроса „Какви мерки според Вас трябва да се предприемат за защита от заплахите за информационната безопасност (възможни са няколко отговора)?" 55% от анкетираните посочват придобиването на лицензно копие на операционната система, 69% - използване на лицензиран приложен софтуер и само 16% посочват използване на криптографски технологии за защита. За сметка на това прави добро впечатление почти повсеместното използване от малкия и среден бизнес на електронни подписи, чиито предимства в ежедневната работа не се нуждаят от коментар. 84% от собствениците и служителите имат и използват електронния цифров подпис при предаването на справки и отчети за централните ведомства, 12% смятат да закупят цифров подпис и само 4% не познават тази технология.

Именно в тази сфера се очертават много големи възможности за развитие на ИТ аутсорсинга в нашата страна, и по конкретно *изнасянето* (сорсването) на услуги, свързани с безопасността.

На анализ се подлагат всички основни компоненти на безопасността: ИТ инфраструктура; хардуер; софтуер; електронни комуникации; безжични мрежи и комуникации.

След обобщаване на събраната информация може да се извърши групиране на информационните обекти в няколко по-големи класове в съответствие с изискванията за достъпност, конфиденциалност и цялостност на данните.

Обикновено пробивите в системите за сигурност на информацията могат да бъдат разпределени в **няколко основни класа**, в зависимост от това какви компоненти на ИТ инфраструктурата са тяхна основна цел:

Хардуерно оборудване – сървъри, работни станции, принтери, дискови носители, мрежови кабели, маршрутизатори, комутатори и т.н.;

Софтуер. На практика всяко приложение, работещо на компютър, включен в корпоративната мрежа е потенциална "врата", за хакерите. Редовното инсталиране на т.нар. "пачове" (Service Pack) за операционните системи, затваря

някои от тези "врати";

Хората. Всички потребители, които имат достъп до устройство включено в мрежата формират "рискова група";

Информацията. Данните, които се създават и използват в корпоративната мрежа, са най-ценният информационен актив за компанията. При срив, приложенията и операционните системи могат да бъдат инсталирани отново, но загубата или разгласяването на данни за клиентите, продажбите и т.н. нанася на бизнеса невъзстановими щети;

Документите. На този много важен за хакерите ресурс, често се отделя недостатъчно внимание. Паролите се записват на хвърчащи листчета, които често са залепени на монитора. Разпечатват се отчети с конфиденциална информация, а после се хвърлят в кошчето за боклук, без да са взети никакви мерки, за да бъдат нечетими. При подобна практика не може да се каже, че компанията има политика за информационна сигурност.

1.4. Уточняване доколко сериозни може да са щетите за предприятието в резултат на атака върху всеки конкретен обект на информационната система

Да се уточни предварително доколко сериозни може да са щетите за предприятието в резултат на атака върху всеки конкретен обект на информационната система е трудно. Все пак има установени правила за изчисляване степента на риска и евентуалните щети, които предприятието може да понесе.

1.5. Анализ на рисковете от нарушение на безопасността в отделни компоненти на системата за електронна търговия

Ключов момент във всяка политика за безопасност е *оценката на риска*. На този етап се изяснява *какво точно защитаваме и от кого*. Разработването на раздела е свързано с идентифициране на ценностите в корпоративната мрежа и проблемите, свързани с тях, които биха могли да възникнат при нарушаване на безопасността.

Под оценка на риска се разбира общия процес на анализ и определяне на риска, а управлението на риска обхваща координирани действия за насочване и контрол на организацията по отношение на риска

Процесът на управление на риска включва няколко фази: идентификация на риска, оценка на риска, отговорности за управлението на риска, докладван на риска и преглед на резултатите. Има разработени стандарти и технологии, с които конкретно се оценява всеки риск и се набелязват мерки за противодействие.[8]

По-горе бяха анализирани подробно основните заплахи за онлайн търговията. Условно може да се разделят на две групи – опасности за предприятието, свързани с работата в Интернет и заплахи, характерни за извършването на сделки в Web. На базата на основните процедури на процеса на електронната търговия от фиг. 6 може да се анализират типовите заплахи и рискове от нарушаване на безопасността при електронната търговия (вж. табл. 1).

[8] Например ISO/IEC 27001:2005, ISO 27002:2005, BS 25999-1:2006, BS 25999-2:2007 и BS 31100:2008.

Таблица 1.

Типови заплахи за онлайн търговията в Интернет

Действия на купувача в Интернет	**Възможни заплахи и опасности**
Купувачът избира продукт или услуга чрез сървъра на електронния магазин и оформя поръчка.	Подмяна на страници на Web сървъра на електронния магазин. Обикновено става чрез преадресация на заявките на купувачите към друг сървър. Това става чрез замяна на записи в таблиците на DNS-сервърите или в таблиците на маршрутизаторите. Много сериозни поражения може да последват, ако клиентът въвежда и номера на кредитната си карта.
Електронната поръчка се предава към базата данни за поръчки на Интернет магазина.	Проникване в базата данни и изменения в процедурите за обработка на поръчки, което може да доведе до незаконно манипулиране с базата данни.
Проверява се дали е достъпен продукта или услугата чрез централната база данни. Ако продуктът не е достъпен купувачът бива информиран. Според типа на магазина, електронната поръчка може да се насочи към друг склад.	Извършване на атаки от типа "отказ от обслужване" и нарушаване нормалното функциониране или извеждане от строя на Web сървъра за електронна търговия.
Ако продуктът е наличен, купувачът преминава към следващата стъпка – потвърждаване на разплащането, а поръчката се разполага в базата данни.	Създаване на лъжливи поръчки от страна на сътрудници на Интернет магазина.
Електронният магазин изпраща на купувача потвърждение на поръчката.	Прехващане на данните, които се предават в системата за електронна търговия между купувача и интернет магазина.
Клиентът извършва електронно разплащане за избраната стока или услуга.	Прехващане на данните за номера на кредитната или дебитната карта на купувача.
Стоката или услугата се доставя на купувача.	Възможни злоупотреби от страна на компанията доставчик или от сътрудниците на Интернет магазина.

Освен рисковете представени в табл. 4 трябва да се държи сметка и за заплахите. Става дума за „традиционни” рискове за безопасността в Интернет като: вътрешни атаки; вируси; спам; отказ от обслужване; други рискове, напр. рискове от частен характер, финансово мошеничество в Интернет и рискове произтичащи от неудовлетворителното решаване на правни и нормативни проблеми.

Всичко се свежда до това да се разработят адекватни и ефективни процедури за безопасност, които да защитят целостта, надеждността и качеството на операциите на електронната търговия и да формират увереност в клиентите по отношение на надеждността на онлайн взаимоотношенията. Именно степента на *увереност на купувачите за безопасността на сделките в Интернет* са един от основните проблеми на електронния бизнес днес.

Целесъобразно е на този етап да се предвидят и *процедури за възстановяване на системата за защита*. За целта трябва да се разработят точни указания и правила за действията, които се предприемат в случай на пробив в системата и за санкциите, които ще бъдат наложени на нарушителите. Обикновен тези правила постоянно се обновяват, за да бъдат адекватни на най-новите рискове и заплахи за безопасността.

3. Тенденции в заплахите за информационната сигурност

Заплахите за информационната сигурност се увеличиха лавинообразно през последните години. След масовото разпространение на компютърни вируси през 90-те години на миналия век, следва появата на други видове вредителски програми, хакерски атаки и други действия, носещи заплахи за информационната сигурност. Обобщавайки мненията на специалисти [9] от водещи компании в областта на ИТ сигурността ще очертаем тенденциите за заплахите за информационната сигурност и най-застрашените области на ИТ за 2011 г. и следващите години.

Основните ИТ области, за които се очаква нарастване на заплахите за информационната сигурност са: „облачните услуги"; социалните мрежи и Web 2.0 услугите; мобилните устройства.

Технологията **„Облачни услуги" (Cloud computing)** представя тенденция за изнасяне на ИТ услуги в чужда инфраструктура („облак"). Тази нова технология за обработване на информацията предизвиква силен интерес сред хакерите и лицата, занимаващи се с индустриален шпионаж. При този вид обработка на информацията софтуерните приложения, които предприятието използва са разположени в чужда инфраструктура. Данните на предприятието също се намират на сървърите на доставчика на услугата, като не винаги е известно, къде точно е тяхното физическо местоположение. Това затруднява много контролът от страна на предприятието – клиент на услугата. Използването на услуга от този вид води след себе си множество заплахи за информационната сигурност на предприятието. Най-често това са загуба на данни или несанкциониран достъп до обработваната и съхранявана информация.

Социалните мрежи и Web 2.0 услугите са сред рисковите области на ИТ сигурността. На първо място, предоставянето на лични данни от техните членове може да доведе до кражба на идентичност. На второ място, включването на потребителите към социалните мрежи от работното място дава възможност за достъп на хакери до корпоративната информация на предприятието.

Социалните мрежи създават отлични условия за работа на създателите на спам предоставяйки удобен начин за неговото изпращане до огромен брой, постоянно увеличаващи се потребители.

От друга страна стремежът към подобряване на предлаганите услуги по мрежата и предоставяне на приложения с по-голяма функционалност увеличава риска за пробиви в сигурността на потребителите на тези услуги.

Мобилните устройства се посочват единодушно от специалистите като платформа, която ще бъде атакувана от хакерите. Тенденцията за увеличаване на дела на тяхното използване (предимно на смартфони и таблети) насочва вниманието на хакерите към този вид устройства. Мобилните устройства предлагат интернет връзка и възможности за комуникация. Напоследък

[9] Grant I. Top 10 IT Security Trends for 2011. ComputerWeekly. http://www.computerweekly.com/Articles/2010/11/09/243805/Top-10-IT-security-trends-for-2011.htm; Top 10 Technology Security Trends for 2011. CIO Update. http://www.cioupdate.com/research/article.php/3917131/Top-10-Technology-Security-Trends-for-2011.htm; Roberts P. Threatpost's Five Security Trends to Watch in 2011. ThreatPost. http://threatpost.com/en_us/blogs/threatposts-five-security-trends-watch-2011-122910; MacDonald N. Six Trends That Will Further Reshape Information Security in 2010. http://blogs.gartner.com/neil_macdonald/2010/01/04/six-trends-that-will-further-reshape-information-security-in-2010/.

значително се увеличава и делът на електронните плащания, извършвани през мобилни устройства. Те също така предлагат все повече услуги като CRM, електронен бизнес и др., което прави тези устройства податливи на атаки. Според PandaLabs чувствително увеличение на заплахите към сигурността ще бъде насочено към операционната система Android, чиято популярност непрекъснато нараства.

За МСП е особено важно да знаят какви заплахи към информационната сигурност могат да очакват в близките години. Това ще им даде възможност да вземат навременни мерки за подобряване на сигурността на техните информационни системи. Най-съществените заплахи към информационната сигурност са хактивистите, социалното инженерство, вътрешните заплахи от страна на служители, проблемите на HTML 5 и т.нар. "Агент в браузъра".

През 2010 г. се наблюдава многократно увеличение на атаките извършвани от хактивисти. **Хактивистите (hacktivist)** са вид хакери, които изразяват кибер протест, който преследва идеологически или политически цели. Няколко хакерски групи организират това движение, имайки за цел да блокират достъпа до Web сайтове на официални организации. На практика Web сайтът се бомбардира със заявки за страници, изпращани непрекъснато от няколко контролирани от хакерите компютъра. Освен хакери с голям опит и познания, в това движение се включват и потребители с по-ограничени възможности, участвайки в тези атаки или в спам кампании.

Социалното инженерство (social engineering) от гледна точка на сигурността е действие, свързано с манипулиране на хората чрез технически средства и „измъкване" от тях на конфиденциална информация. Целите на социалното инженерство са получаване на несанкциониран достъп до системи или информация с цел измама, нарушаване на работата на мрежата, индустриален шпионаж, кражба на идентичност, нарушаване работата на компютърната система или мрежа. Социалните мрежи с техните милиони потребители са много подходяща среда за тези кибер престъпници. Потребители им са изложени на по-големи заплахи за сигурността в сравнение с потребителите на другите комуникационни услуги. Очаква се основната заплаха да бъде насочена към потребителите на двете най-големи социални мрежи Facebook и Twitter.

Вътрешните заплахи показват тенденция на нарастване през 2010 г., като се очаква това да се запази и през следващите години. Те се дължат на масовите уволнения на служители резултат от икономическата криза. Това действие води до недоволство сред служителите, които неправомерно „взимат" със себе си информация на фирмата с цел да я предадат на конкурентите и по-лесно да си намерят нова работа.

Технологията **HTML 5** поставя някои нови проблеми, свързани със сигурността. HTML е последният комплект от стандарти за описание и показване на Web страници, одобрен от консорциума Worl Wide Web. HTML 5 предоставя много допълнителни възможности. Web браузърът може да управлява Web приложения, а не само Web страници както беше в предишните версии. Това ще доведе до възможност за нови атаки, които ще се увеличават паралелно с налагането на стандарта HTML 5.

„Агент в браузъра" (Man in the browser (MiTB)) е нов вид атака насочена предимно към банковата система. Злоумишлените действия се извършват на компютъра на клиента с помощна на зловредна програма (троянски кон), която заразява неговия Web браузър. Тази зловредна програма

може да модифицира страници и съдържанието на транзакции, краде удостоверения на потребителя за свързване, банкови сметки и друга финансова информация. Този вид атака е особено опасна за банковите операции и за съжаления обикновено не се открива от антивирусните програми.

Заключение

В заключение може да се направят няколко основни извода.

Първо, електронната търговия обединява множество различни функции, базирани на използването на съвременни ИКТ като нови технологии за организиране на контактите между купувачи и продавачи, методи за представяне, обсъждане и формиране на поръчките, определяне условията на сделката, реда за продажбата на стоки и услуги и процесите за осъществяване на онлайн разплащанията. От тук и извода, че решаването на проблемите на безопасността, преди всичко изисква решаване на проблемите, свързани със *защитата на информационните технологии*, които се използват за реализирането й.

Второ, има много основания да се твърди, че *информационната среда на малките и средни фирми е по-уязвима* към пробиви в сигурността. Въпреки това проблемите на безопасността на малкия и среден бизнес в нашата страна силно се подценяват. Усилията се насочват основно към разработването и функционирането на сайта като се пропускат в стратегията проблемите на безопасността на търговските онлайн процеси. По този начин от самото начало не се отчитат някои основни изисквания за резултатна електронна търговия и това впоследствие се отразява негативно върху начинанията. Причините се коренят в силно ограничените средства за ИКТ и закупуване на съвременно мрежово оборудване и технологии за защита. Традиционна се *омаловажава на ролята и значението на ИКТ и безопасността*, тяхното решаване се оставя на последно място в приоритетите като в повечето случаи липсва ясна перспектива и дългосрочно стратегия. Омаловажават се щетите, които персоналът може да причини на МСП в качеството си на най-непредвидимата и неконтролируемата уязвимост за сигурността, и не се инвестира в обучение и повишаване на информационната култура на служителите.

Трето, в предлаганата методика е направен опит да се обобщи съществуващия опит в областта на безопасността на електронната търговия и да се предложи подходящо решение за малки и средни предприятия. В нея има няколко основни момента – а) ясно очертаване на целта и задачите на политиката за безопасност, б) анализ и оценка на ресурсите, които трябва да бъдат защитени; в) идентифициране на потребителите, ползващи различните ресурси; г) класификация на уязвимите места и определяне на най-вероятните източници на заплаха за всеки ресурс; д) тестване, документиране и оптимизация на политиката за сигурност.

Четвърто, разработването и практическата реализация на методиката за безопасност на електронната търговия е целесъобразно да се възложи на външна организация. По много причини малките и средни предприятия не са в състояние удовлетворително да решават целия комплекс от проблеми, свързани с безопасността на бизнеса в Интернет. Засега в нашата страна ИТ аутсорсингът не е много популярен в малкия и среден бизнес, но с разрастване на инициативите за онлайн търговия и все по-мащабното навлизане на ИКТ в тази сфера, може да се очаква преориентация към повишено търсене на ИТ услугите на външни компании.

РЕЗЮМЕ:

В статията се предлага подход за създаване на **политика за безопасност** на електронната търговия в МСП, която е базирана на няколко принципни положения: идентификация и автентификация; съхраняване на данните; обработка на поръчките; постепенност и етапност; използване на водещи технологии и доказани решения в областта на електронната търговия; защита на инвестициите; защита на транзакциите.

Анализира се съдържанието на **всяка една от основните фази**, през които преминава разработването на политиката за безопасност в МСП: уточняване на целите и задачите на политиката за безопасност на електронната търговия; анализ на информационните обекти и потоци, които трябва да се защитават; анализ на текущото състояние на системата за информационна безопасност в предприятието; класифициране на обектите, които се нуждаят от защита; уточняване доколко сериозни може да са щетите за предприятието в резултат на атака на ИС; анализ на рисковете от нарушение на безопасността в отделни компоненти на системата за електронна търговия; разработване на рамките на политиката за безопасност; финансови разходи за реализирането на политиката за безопасност; тестване, приемане, документиране и оптимизиране на политиката за безопасност.

ONE APPROACH TO POLICY FORMATION OF SAFETY AND SECURITY OF DATA IN SMALL AND MEDIUM ENTERPRISES

Abstract

The article offers an approach to establishing the safety policy of e-commerce in SMEs, which is based on several principles: identification and authentication; data storage; orders processing; description of the performance, usage of the leading technologies and proven solutions in electronic commerce; investment protection; security of the transactions.

The content of each of the key phases through which the development of safety policy in SMEs passes is analyzed: clarification of the goals and the aims of the safety policies of the electronic commerce; analysis of the information objects and flows that must be protected; analysis of the current state of the information security system in the enterprise; classification of the objects that need protection; specification how serious the damages may be for the enterprise in a result of the attack of IP; analysis of the risks of security breach in the individual components of the system for e-commerce; development of the safety policy; financial costs of implementing the policy for safety; testing, acceptance, documentation and optimization of the safety policy.