Erasmus+

Проектът се финансира от Европейската комисия по програма **Еразъм+, Ключова дейност 2: Сътрудничество за иновации и обмен на добри практики, Дейност: Стратегически партньорства в сферата на младежта**

DiFens

Електронно ръководство

За млади предприемачи

Добре дошли!

Драги млади предприемачи, добре дошли в електронния наръчник на DiFens!

По-долу ще намерите информация, примери, съвети и начини как да подкрепите бизнеса си в дигиталната ера. Експерти, в различни области, съставиха този наръчник в пет отделни части, които да бъдат кратки, точни и полезни за вас, с фокус върху пет основни области, свързани с дигиталната сигурност на бизнеса:

В **Част 1** ще намерите някои уводни, но също така задълбочени инструкционни бележки за това какво е бизнес дигитализация, как и къде да се прилага и защо, и кои инструменти могат да ви бъдат от полза в този процес.

В **Част 2** ви очаква информация относно социалните иновации, социалното предприемачество, ползите и предимствата на социалните предприятия, както и специфичните заплахи и възможности, които биха могли да произтекат в тези сфери на дейност.

Част 3 насочва вниманието към правните аспекти за закрила на дигиталния бизнес, по-специално въпросите за защита на личните данни, защита на потребителите, електронната търговия и бисквитките.

Части 4 и 5 се отнасят до заплахите за киберсигурността като обясняват какви са те и как да се справим с тях, очертавайки цялостна стратегия, която да използваме.

Всяка част включва подобни части – в различни точки, разделите дават информация, примери и съвети. Освен това в края на всеки раздел има **контролен списък**, свързан с темата, който да помогне за проверка на издръжливостта на бизнеса спрямо тази нова информация, **препоръки за допълнителни материали по темите**, за допълнителни знания по темата, както и **терминологичен речник**, който може да бъде отварян винаги, когато потокът от информация е твърде бърз.

Съдържание

ЧАСТ I

ДИГИТАЛИЗАЦИЯ НА БИЗНЕСА

Списък със съкращения

Абревиатура	Значение
CEO	Chief Executive Officer
IoT	Internet of Things
BI	Business Intelligence
ROI	Return on Investment
CRM	Customer Relationship Management
IT	Information Technologies
URL	Uniform Resource Locator
CIO	Chief Information Officer
GPS	Global Positioning System
QR code	Quick Response Code
ERP	Enterprise Resource Planning
SQL	Structured Query Language
DAP	Digital Adoption Platform
POS	Point of sale
SLA	Service Level Agreement
AI	Artificial Intelligence
APIs	Application Interfaces
OWASP	Open Web Application Security Project

CA	Computer Associate
USB	Universal Serial Bus
SMEs	Small and Medium-sized Enterprises
RFID	Radio Frequency Identification
HR	Human Resources
ICT	Information and Communication Technology

A. Въведение

Бизнесът, изправен пред Дигиталната Ера

Светът е по-взаимосвързан от всякога. Възможността за потапяне във високо октанова, с голям обем и постоянно променяща се реалност започва да се трансформира в необходимост както за предприемаческите модели, така и за предприемачите. Проникването на технологиите в света на бизнеса не се поставя под въпрос вече. Основните характеристики, които трябва да бъдат разгледани са иманентната предстояща промяна на природата на бизнеса, която се утежнява от работните навици на поколението „Millennials". В настоящата глава следва да бъдат разгледани много от основните въпроси, сред които и някои от основните стълбове на бизнес дигитализацията.

Всеки съвременен бизнес трябва да балансира растежа, поеманите рискове и персонала си по съответен начин. Ако растежът е ефективен, то тогава „излитането" става възможно. Въвеждането на технологии за повишаване на продуктивността и на гаранции за планирането на бизнеса води до понижаване на възможните рискове. В другия край на този спектър се намират потребителите и служителите на предприятията. Тук е важно да отбележим, че лесният достъп се пресича с продуктивността, когато едно предприятие въведе и приложи някои нови технологии, както и подобряването на качеството на живот, които те носят.

Конкурентоспособност

На ръба. Живеем, работим, правим бизнес „на ръба", в хармония с дългосрочното планиране отвъд предписаните хоризонти, това ни поддържа гъвкави. Създаването на конкурентно предимство и преследването на тази цел до край е стратегията, която илюстрира сбор от много действия. Най-важната стъпка е правилното позициониране от ден първи. Да се отличиш от тълпата като авторитет, експерт, лидер може да доведе до значителни промени докато компанията се разраства. Цифровата ера изисква дълбока революция.

Казват, че не е нужно да се преоткрива колелото. Следването на ясна мисия, която отразява нуждите на постоянно менящия се пазар, е ключово. Постоянният

анализ на конкуренцията и клиентите може да даде възможност на бизнеса да остане фокусиран. Развитието на клиентите е реална нужда. Освен това, подпомагането на развитието на хората зад кулисите, тяхното водене и вдъхновяването им, се явява също толкова важна основа в развитието на един бизнес. В тези случаи умението да бъдеш иновативен през цялото време подпомага предприемача за неговото безопасно развитие в гореспоменатите сектори.

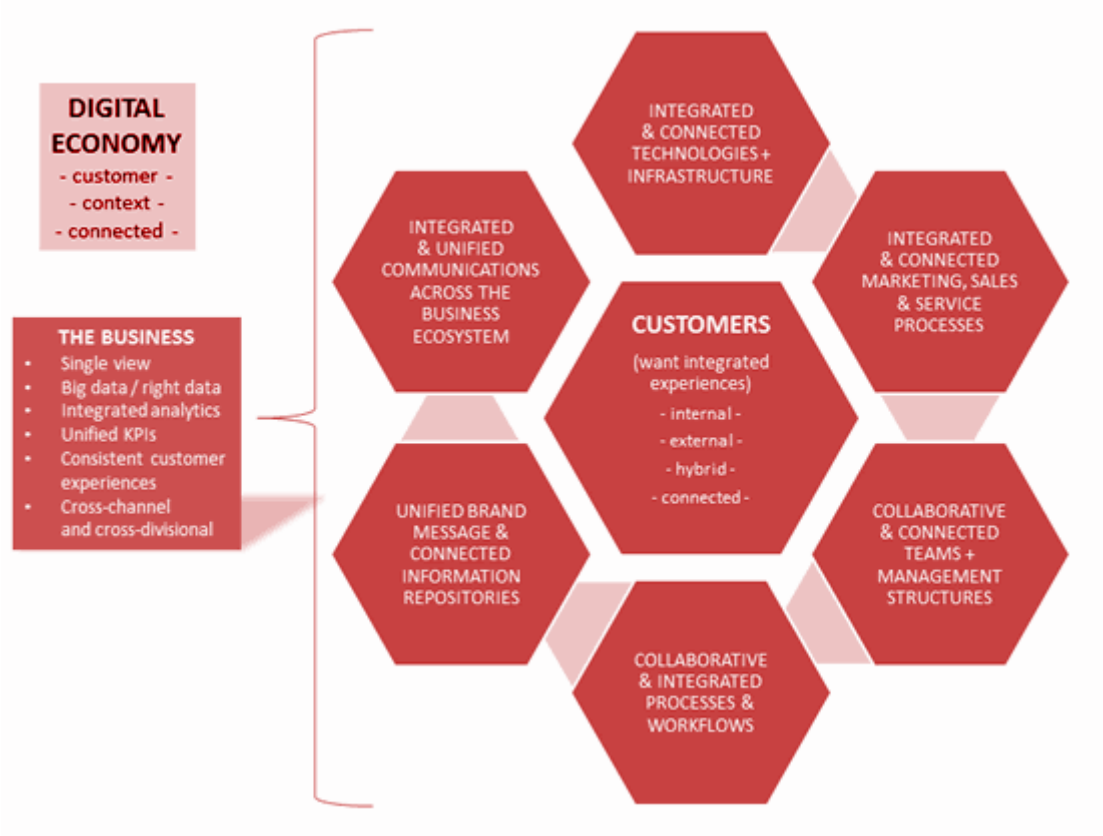
Нуждата от адаптация

Еволюцията естествено следва натрупването на опит. Всички умни хора се учат от своите грешки, а по-умните съумяват да се учат от грешките и от победите на другите. Промяната винаги носи със себе си известен риск, но понякога нежеланието ни да рискуваме води до пораждането на най-сериозните рискове.

Понастоящем 80 процента от компаниите вече осъзнават, че прилагането на технологиите в своите дейности е от ключово значение за техния успех, имайки предвид, че Четвъртата индустриална революция вече чука на вратите ни. Въпреки това, само 29 процента от тях заявяват, че вече са въвели управленските и технологичните решения на новото хилядолетие.

Цифровата ера предизвика революция в света на бизнеса. В наши дни трябва на първо място да си иновативен, за да можеш да бъдеш и конкурентен. Приспособяването към всички тези промени по находчиви начини и преди започване на технологичната надпревара е в състояние да отличи един бизнес от всички други.

Очевидният извод, който трябва да се направи, е че всички тези мерки са породени и засилени вследствие на бизнес дигитализацията.

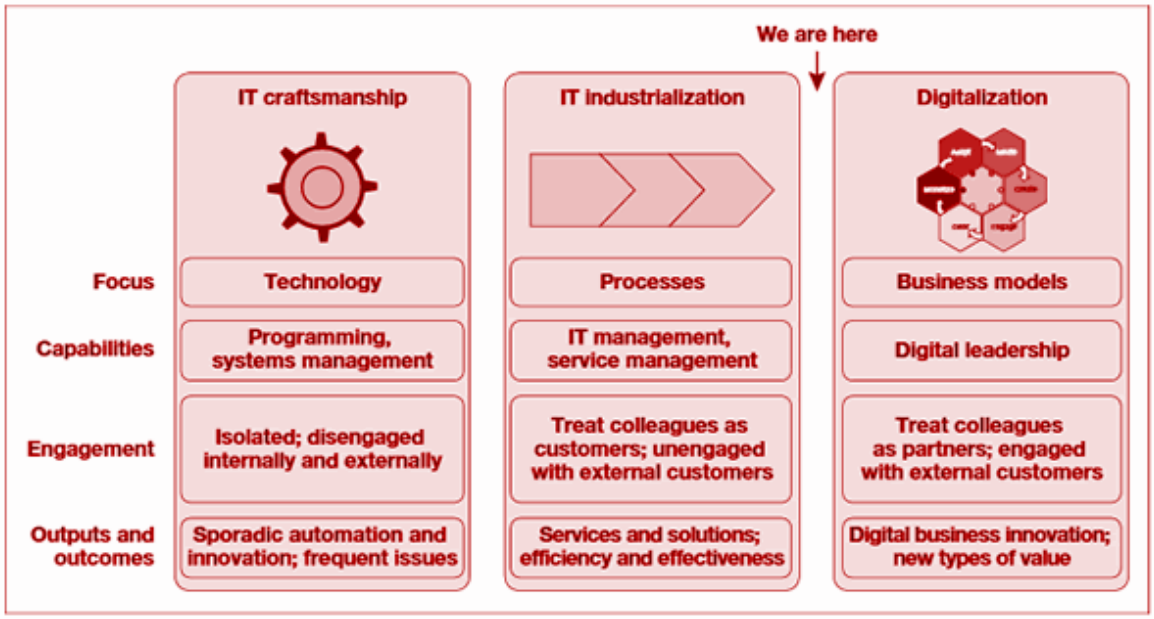


Фигура. 1: Бизнесът в дигиталната икономика

Какво е бизнес дигитализация?

Макар често дигитализацията да се използва в смисъл на цялостна дигитална трансформация, в действителност тя е нещо съвсем друго.

Дигитализация означава използването на дигитални (цифрови) технологии и данни (напълно и относително дигитални) с цел създаване на приход, подобряване на бизнеса, замяна/трансформиране на бизнес процесите (не просто чрез тяхната цифровизация) и създаване на среда за дигиталния бизнес, в чиято основа е цифровата информация. И тъй като имаме 3 дефиниции, нека най-добре да изясним в какъв смисъл се използва терминът.



Фигура 2: История и хронология на бизнеса

По отношение на бизнеса, дигитализацията най-често се отнася до разрешаването, подобряването и/или трансформирането на бизнес операции, и/или бизнес функции, модели/процеси, както и други дейности, чрез прилагането на механизмите на дигиталните технологии и по-широкото им използване в контекста на цифровизираните данни, които превръщат тези знания в такива със специфична полза. Това изисква дигитализация на информацията, но последната е с голямо значение и в нейната основа стоят данните. И докато дигитализацията се отнася предимно до системите за запис на информация, то в крайна сметка към нея се причисляват и вътрешните системи, както и системите за ангажираност, които използват цифровизираните данни и процеси.

Вторият аспект, който често се споменава, се състои в това, че дигитализацията се разбира като специфична „среда“ в областта на бизнеса. Вземете например дигиталните работни места. Често чрез работата в такава среда се стремите да ограничите използването на хартия до минимум, но дигиталната работна среда обхваща също така и други неща. Използването ѝ означава, че вашата работна сила работи по различен начин, използвайки инструменти като мобилните устройства и други технологии, които позволяват на служителите ви да са мобилни и/или прилагането на социално сътрудничество и унифицирани

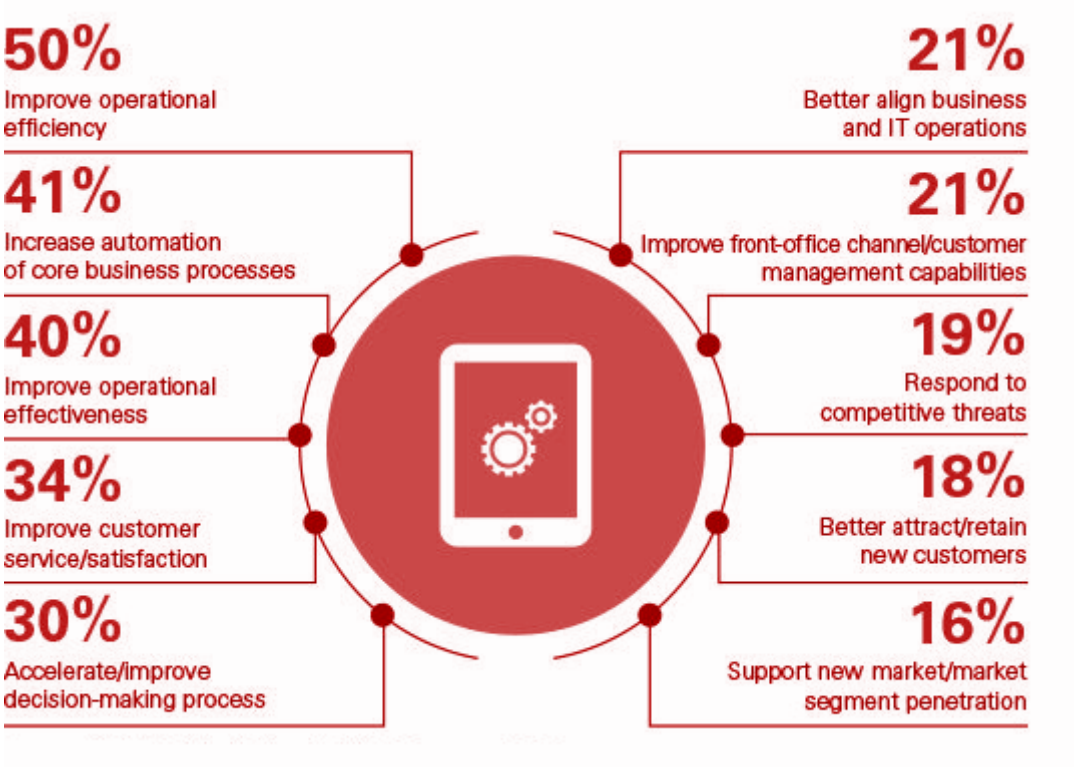
платформи за комуникация, представляващи дигитални системи, които позволяват на служителите ви да работят по “по-дигитален начин”. Това, от друга страна, създава много възможности за различен начин на действие и изисква повече от простото наличие на дигитализирани данни.

Дигитализирането на вашия бизнес води до създаването на различен, дигитален бизнес. Списъкът с нещата, които можете да дигитализирате (вериги за доставки, които се превръщат в дигитални вериги за доставки и др.), е дълъг. Погледнато по-общо, дигитализацията се разглежда като пътя за развитие на дигиталния бизнес и дигиталната трансформация, както и като процес по създаване на нови – дигитални – приходни потоци и други приноси при извършването им. Процесът по дигитализация изисква сериозна промяна, ето защо много хора взаимнозаменяемо използват дигитализацията и дигиталната трансформация (както и ние правим често).

Третото значение на термина дигитализация се простира извън бизнеса и се отнася до непрекъснатото приемане и използване на цифровите технологии във всички сфери на социалните и човешки дейности. Помислете например за увеличаващият се брой дигитални потребители, развитието на дигиталното здравеопазване, нарастващата дигитализация на правителствените услуги, на маркетинга, на потребителските услуги и други. Казано с други думи: цялостната дигитализация на услугите (във всички възможни сфери).

[I-scoop.eu. (2018). *Digital business: transformation, disruption, optimization, integration and humanization*. [online] Available at: https://www.i-scoop.eu/digital-business]

Ползи от дигитализирането на вашето предприятие



Фигура. 3: Най-забележими ползи от дигитализацията

Колкото и смешно да звучи, “базисен” е термин, който описва 20 процента от малките предприятия в САЩ, които не използват дигитални инструменти за развитие на своите предимства. В тази връзка проучването на изданието „Deloitte“ относно свързаните малки предприятия изследва как дигиталните инструменти подпомагат дейността на малките предприятия и чрез това и икономиката на САЩ. В проучването собствениците на малките предприятия са класифицирани в четири отделни групи в зависимост от степента на тяхната дигитална ангажираност и по-специално от това доколко те използват дигитални инструменти в тяхната дейност. Ето и направените изводи:

- Базисен (20 процента): Малките предприятия на това ниво са с недостатъчно развито дигитално присъствие. Те разчитат на традиционните методи за маркетинг, като например целево рекламиране чрез имейли и печатни реклами. Тези предприятия няма уебсайт и не са активни в социалните мрежи, като единствения дигитален инструмент, който използват, се оказва имейл адресът.

- Междинен (30 процента): Малките предприятия на това ниво използват дигитални инструменти като например обикновен уебсайт (без електронни реклами или мобилни възможности). Те използват някои основни онлайн маркетингови инструменти - включване в онлайн справочници или използване на онлайн пазари на трети страни.
- Висок (30 процента): Тези предприятия вече разполагат с по-модерен уебсайт, с мобилна версия, в който могат да се правят онлайн резервации или чрез който може да се извършва онлайн търговия. Те се разпространяват чрез множество активности в множество социални мрежи и канали за онлайн търговия, а също така използват вътрешни дигитални инструменти като видео конференции или облачен софтуер, с цел повишаване на производителността и ефективността в дейността им.
- Напреднал (20 процента): Тези наистина дигитални предприятия вече използват всички горепосочени дигитални инструменти, но на по-високо ниво. В допълнение следва да отбележим, че те използват и по-усъвършенствани дигитални инструменти – например разработване на мобилно приложение или анализиране на данни, чрез които да се научат предпочитанията на потребителите и тенденциите при продажбите на стоки.
- Проучването установи, че колкото повече се използват дигиталните инструменти, толкова по-големи са ползите за едно предприятие. В тези случаи е без значение от колко време сте в бизнеса, къде се намира предприятието ви или дори в коя сфера сте. Независимо от това, разликата между постиженията на основните, напредналите (наистина дигиталните) малки предприятия е огромна. Имайте предвид, че:

Малките дигитални предприятия създават работни места. При тях е почти три пъти по-вероятно да са открили нови работни места през изминалата година в сравнение с обикновените предприятия. Друг интересен факт е, че има тенденция тези служители да са по-продуктивни от служителите в обикновените предприятия, благодарение на вътрешните дигитални инструменти, които компанията използва.

Малките дигитални предприятия достигат до нови пазари. Благодарение на непрекъснатото разширяване на пазарните възможности, те са в състояние да достигнат до много по-широк кръг от потребители и в резултат на това статистиката сочи, че е три пъти по-вероятно такива дигитални предприятия да са извършвали износ на продукт или услуга през последната година в сравнение с обикновените (недигитални) предприятия. Повече от четиридесет процента (43 процента) от клиентите на малките дигитални предприятия са регионални, национални или международни в сравнение със само 28 процента при обикновените предприятия.

Малките дигитални предприятия са иноватори. Вероятността високо технологичните и напреднали дигитални предприятия да са представили нов продукт или услуга в последната година е почти 10 пъти по-висока в сравнение с вероятността при обикновените предприятия.

Малките дигитални предприятия достигат до повече потребители. През изминалата година вероятността тези предприятия да са завишили броя на запитванията към тях за продажби е три пъти по-висока в сравнение с тази на обикновените предприятия. Нещо повече, малките дигитални предприятия изпитват осезаемо по-висока активност от клиентите в рамките на целия процес по извършване на продажби – от наличието на интерес до запитвания за продажби.

Като се вземат предвид всички тези фактори, които са в тяхна полза, не е учудващо, че тези малки дигитални предприятия се разрастват с бързи темпове. Сравнени с обикновените малки предприятия, през предишната година дигиталните предприятия имат два пъти по-високи приходи за всеки служител, като се отчита четири пъти по-висок общ ръст на приходите. Развиващите се пазари, иновативните продукти и услуги, както и разширяващият се кръг от потребители съвсем нормално в крайна сметка водят до разширяване на дейността на тези предприятия.

За да обобщим казаното дотук, ако едно предприятие иска да се развива или дори само да оцелее, то трябва непрестанно да подобрява начините, по които използва дигиталните си инструменти и останалите си разнообразни процедури.

[Small Biz Daily. (2018). *The Benefits of Being a Digital Business - Small Biz Daily*. [online] Available at: https://www.smallbizdaily.com/benefits-digital-business/].

Другата страна на монетата

Ако това да бъдете дигитално предприятие е идеалната ситуация и безотказна формула за успех, защо тогава вече всички предприятия не са поели по пътя на дигиталната трансформация? Всъщност може и вече да са го поели. Процесът по дигитализация често е труден и изисква значително време и усилия, като може също така да крие доста опасности и препятствия, които да не позволят на много предприятия да осъществят така желаната трансформация. Нещо повече, поддържането на едно дигитално предприятие може и да не е толкова лесно, тъй като заплахи за неговата сигурност могат да се появят дори след завършването на процедурата по трансформацията му, в хода на обичайната му дейност.

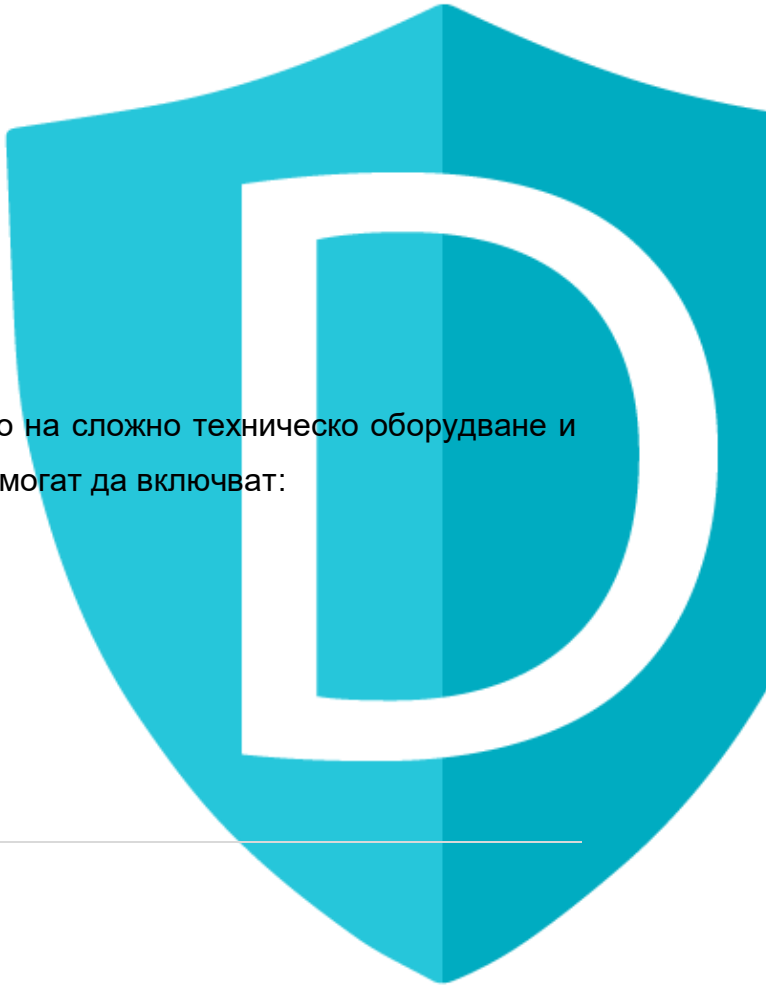
Дигитални заплахи за вашия бизнес

Докато Интернет, мобилните мрежи и онлайн рекламирането могат да помогнат на малките компании в борбата им с по-големите им съперници, използването на тези дигитални инструменти може да доведе и до наличието на значителни рискове:

- Измами с транзакции
- Досадни нарушители
- Вътрешна работа (саботаж)
- Некачествен софтуер
- Мобилни устройства

Други проблеми, свързани с използването на сложно техническо оборудване и по-иновативни дигитални бизнес модели, могат да включват:

- Атаки на устройства тип (IoT)
- Сигурност на данните
- POS атаки



[Forbes.com. (2018). [online] Available at: https://www.forbes.com/2007/06/14/microsoft-apple-symantec-ent-tech-cx_df_0614riskdigital]

Изображение. 4: Дигитални заплахи за бизнеса

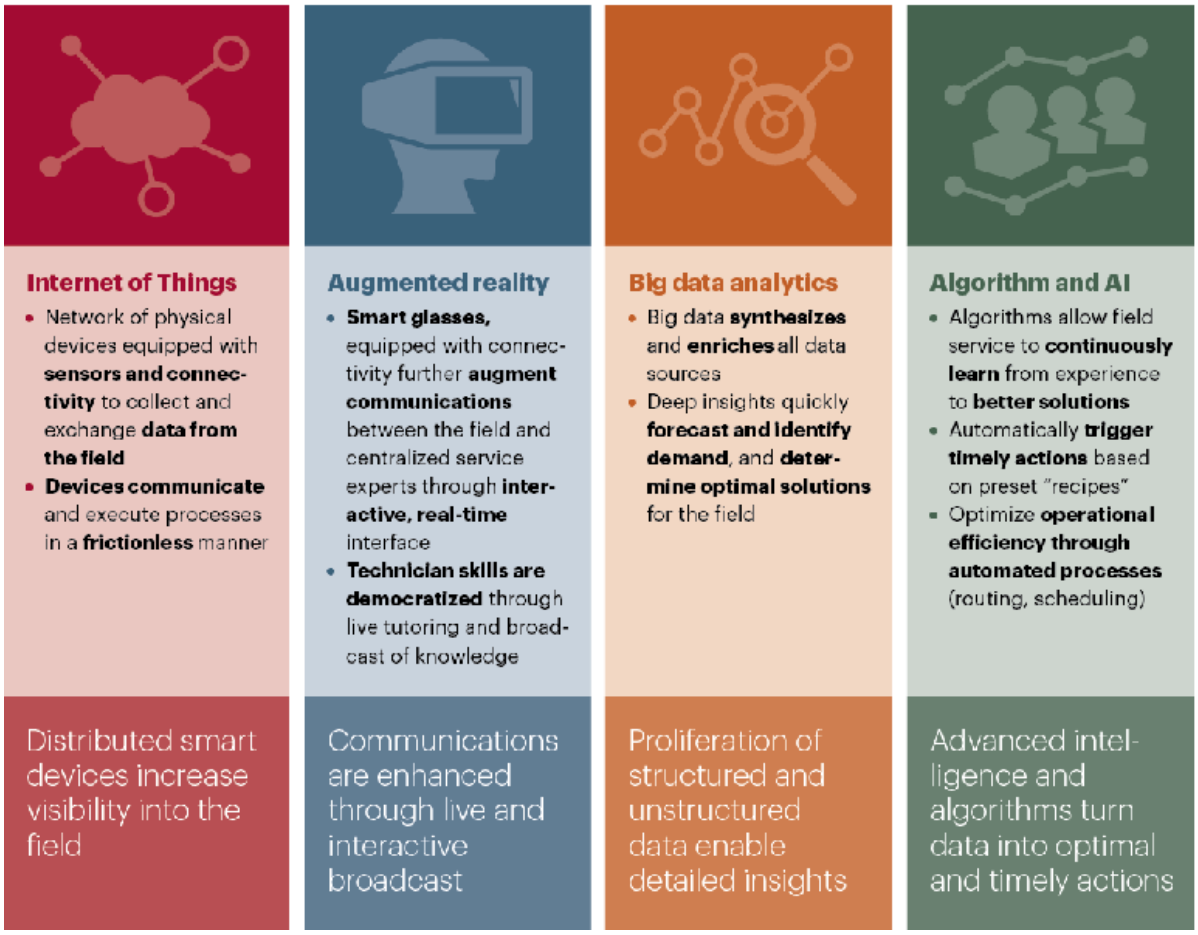
Дигиталните технологии в условията на бизнес дигитализация

Дигиталните технологии са един от най-важните фактори за подобряване на икономиката на страните. Благодарение на тях, в тези страни се създават нови работни места, повишава се стандартът и качеството на живот на хората и по този начин се полагат основите на едни по социално отговорни и екологични общества. Граждани, предприятия, университети и правителства подобряват непрестанно връзката помежду си в условията на днешния дигитален свят. Дигитализирането в своята същност променя живота на хората: променя начина, по който те работят, пазаруват, социализират се, общуват и се образоват. То също така прекроява облика на традиционните индустрии и предизвиква значителни промени в бизнес средата на всички отрасли – от мода до автомобилостроене, от транспорт и логистични услуги до електроразпределителни услуги. Нещо повече, новите технологии вече се разработват много по-бързо и вследствие на това се наблюдава и сериозно подобрение в начина, по който иновативните продукти и услуги се замислят,

разработват, произвеждат и разпространяват. Развитието на тези технологии играе ключова роля, за да може бизнесът и предприятията да се подобряват и да изкарват своевременно на пазара иновативни продукти и услуги, чието експедитивно разработване е било невъзможно преди. Дигиталните технологии подпомагат преобразуването на веригите за създаване на стойността на продуктите, подобрява процесите по проучване на пазара, повишава нивото на ефективност, намалява сроковете за пускане на продукти на пазара и увеличава удовлетвореността на потребителите. В допълнение можем да посочим, че с помощта на съвременните технологии малките и средни предприятия (SMEs) вече могат да се разпространят глобално от момента на създаването си, като по този начин достигат до чуждестранни пазари и потенциални таланти непрестанно. Поради това не е учудващо, че организациите се разрастват два или три пъти по-бързо в случаите, когато последните използват активно дигитални технологии в сферата на работата си.

Модерните технологии за сътрудничество не само дават възможност за достигането до много по-широк и разнообразен кръг от потенциални таланти, до които стартиращият или разрастващият се предприемач има поглед; те позволяват на тези талантливи личности да работят заедно по определен глобален проект, независимо от факта, че последните се намират в различни часови зони и географски ширини.

Две от новите дигитални технологии, с нарастващо значение за бизнеса, са облачните изчисления и големите информационни масиви.



Изображение 5: Новите възможности, които дигиталните технологии предоставят

B. Облачно базирани решения – функционалности и заплахи

Изчислителни облаци (cloud computing) в бизнеса

Изчислителните облаци осигуряват възможност на предприятията да управляват своите компютърни ресурси онлайн. Терминът промени значението си през последните няколко години, като може да се използва и за означаване на използването на трета страна за съхраняване на вашите данни и други компютърни нужди. „Облакът" се отнася до Интернет, а извършването на операции „в облака“ описва начина, по който предприятията съхраняват и получават достъп до данните си чрез Интернет връзка. Изчислителните облаци позволяват на предприятията да имат достъп до информацията си виртуално, създавайки гъвкав и глобален начин за достъп до данните ви по всяко време.

Изображение 6: Изчислителни облаци в бизнеса

Какво са изчислителните облаци (cloud computing)?

Интернет променя начина, по който правим бизнес и общуваме като общество. Обичайно хардуерът и софтуерът се съдържат изцяло на компютъра на потребителя. Това означава, че вашият достъп до данните и програмите ви се извършва само и единствено чрез вашия собствен компютър.

Изчислителните облаци ви дават възможност да имат достъп до тези ваши данни и програми, макар и да сте извън вашата компютърна среда. Вместо да съхранявате вашите данни и софтуер на личния си компютър или сървър, последните се съхраняват на „облак“. Това може да включва приложения, бази данни, имейли и файлови услуги. Като пример за изчислителни облаци можем да посочим отдаването под наем срещу закупуване. Това по същество представлява наемане на определено пространство (сървърно пространство или достъп до софтуер) от доставчик на облачни услуги и използването му чрез Интернет. Вместо да купувате ваши собствени компютърни съоръжения, вие наемате последните от доставчик на услуги, като му плащате само за ресурсите, които използвате.

Изчислителните облаци биват 4 вида, в зависимост от различното ниво на достъп и настройките за сигурност. Преди да прехвърлите вашите данни на облака, първо следва да прецените кой вид облак отговаря напълно на нуждите на вашия бизнес.

Частен облак

При частния облак услугите и инфраструктурата се поддържат и управляват само от вас или от трета страна. Тази възможност намалява потенциалните рискове за сигурността и ги контролира, като подобен облак ще пасне на вашите нужди в случай, че вашите данни и приложения представляват съществена част от вашия бизнес и поради това се нуждаете от по-високо ниво на сигурност или от определени изисквания за чувствителни данни.

Общностен облак

Общностен облак е налице, когато няколко организации споделят общ достъп до частен облак, при сходни съображения за сигурност. Например, няколко франчайз компании използват свои собствени публични облаци, но последните се поддържат дистанционно в частна среда.

Публичен облак

Публичният облак представлява такъв облак, при който услугите се съхраняват и управляват от външна организация, доставчик на облачни услуги, като Google или Microsoft, а достъпът до тях се извършва по Интернет. Тази услуга предоставя най-доброто ниво на гъвкавост и спестяване на разходи, но е по-уязвима от частните облаци.

Хибриден облак

Хибридният облак е такъв вид облак, който съвместява предимствата както на частните, така и на публичните облачни услуги. Чрез разпределянето на вашите възможности към различните видове облаци, вие извличате ползите от всеки един.

Например можете да използвате публичен облак за съхранение на вашите имейли, за да спестите сериозни разходи по съхранение, а в същото време да съхранявате чувствителните си данни сигурно в частен облак.

Как работят изчислителните облаци

Съществуват 3 основни модела за доставка на изчислителни облаци, които са по-известни като:

- Софтуер като услуга (SaaS)
- Инфраструктура като услуга (IaaS)
- Платформа като услуга (PaaS)

В зависимост от вашите нужди, вашето предприятие може да използва един от тези модели на услуги, както и смесица между трите модела.

Софтуер като услуга (SaaS)

SaaS е най-известната форма на облачни изчисления за малки предприятия. При този модел вие имате достъп до поддържани чрез Интернет софтуерни приложения, като използвате браузър, за разлика от обикновените приложения, които се съхраняват на вашия компютър или сървър. В тези случаи хостът на софтуерното приложение е отговорен за контролирането и поддържането на приложението, включително за неговите софтуерни актуализации и настройки. Вие, в качеството си на потребител, имате само ограничен контрол върху самото приложение и настройките за конфигурация.

Типичен пример за SaaS представляват уеб базираните имейл услуги или системите за управление на връзките с клиенти.

Инфраструктура като услуга (IaaS)

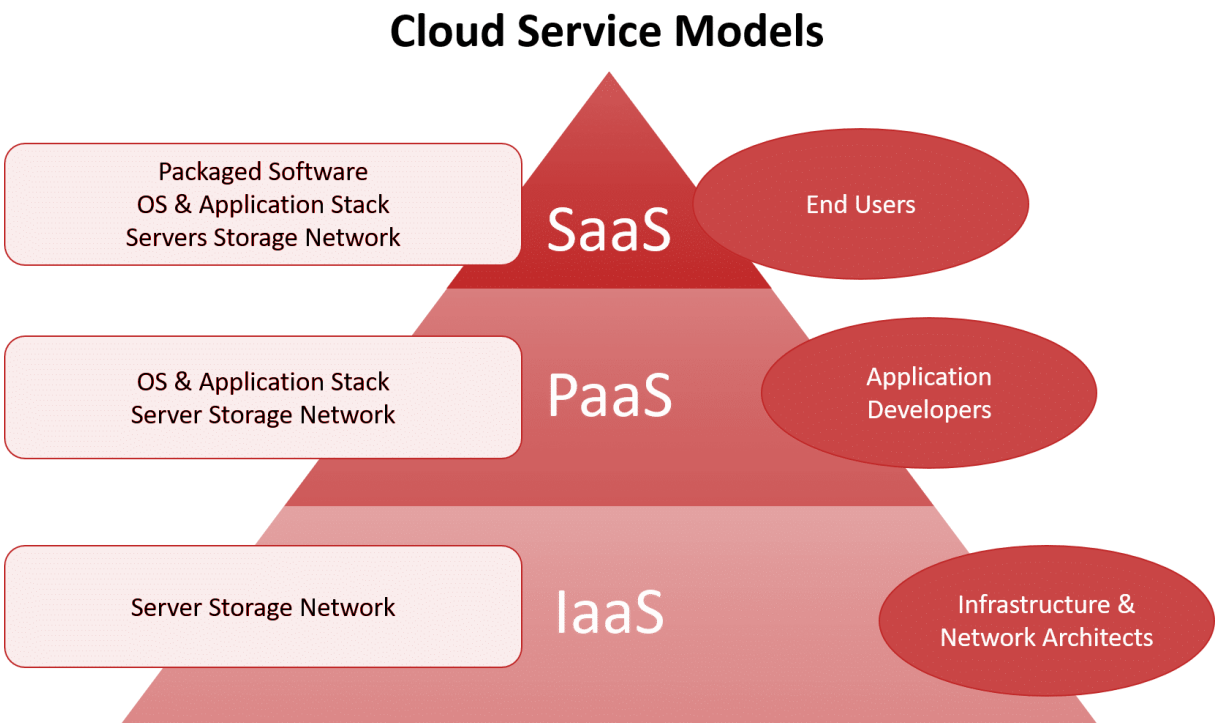
IaaS типично се означава като купуване или отдаване на вашите компютърни мощности и дисково пространство от външен доставчик на услуги. Тази възможност ви предоставя достъп до данните ви чрез частна мрежа или чрез Интернет. В тези случаи доставчикът на услуги поддържа физическия компютърен хардуер, включително компютърната обработка, паметта, съхранението на данни и мрежовата връзка.

Като примери за IaaS се посочват Amazon EC2, Rackspace and Windows Azure.

Платформа като услуга (PaaS)

PaaS може да бъде описана като съчетание между SaaS и IaaS. При нея вие наемате хардуера, операционните системи, съхранението и капацитета на мрежата, която IaaS осигурява, както и софтуерните сървъри на приложенията. PaaS ви предлага повече контрол върху техническите аспекти на вашите компютърни настройки и възможност за тяхното променяне в зависимост от вашите нужди.

[DreamHost. (2018). *What is Cloud Computing? Can It Help Your Business? - DreamHost.blog*. [online] Available at: https://www.dreamhost.com/blog/cloud-computing-for-business]



Img. 7: Cloud Service Models

Каква е ползата от изчислителните облаци за предприятията?

Изчислителните облаци могат да ви предоставят много ползи. Те ви позволяват буквално да създадете свой виртуален офис, за да имате гъвкавостта да се свързвате с бизнеса си навсякъде и по всяко време. С нарастващия брой на уеб свързани устройства, които се използват в настоящата бизнес среда (например смартфони и таблети), достъпът до вашите данни е дори по-лесен. Нека разгледаме по-подробно 8 начина, чрез които изчислителните облаци могат да бъдат от полза за вашите предприятия:

Опростеност

Инсталирането на нов софтуер, информирането относно проблеми със сигурността, инсталирането на пачове и обновяването на софтуерите до по-нови версии е работа на пълен работен ден. Въпреки това много малки предприятия не могат да си позволят да назначат вътрешен компютърен специалист, което ги принуждава да наемат външни ИТ консултанти, които често са заети и невинаги

могат да посрещнат нуждите на предприятието. Други предприятия пък разчитат на неволни ИТ специалисти като офис мениджъра на компанията например.

Тези подходи водят до загуба на време, пари и възникване на спречквания, като в същото време могат да изложат сигурността на вашето предприятие на риск. Ако вашето предприятие няма назначен ИТ специалист сред служителите, то тогава използването на облачно базиран софтуер може да улесни живота ви значително. При използването му всички необходими актуализации се извършват автоматично от доставчика на облачни услуги, който разполага с цял екип от ИТ експерти, имащи за цел да предоставят на потребителите най-новите възможни технологии. Дори и вашето предприятие да има назначен ИТ специалист сред служителите, използването на доставчик на облачни услуги дава възможност на вашите компютърни специалисти да прекарват по-малко време върху решаване на проблеми и поддържане на системата, като по този начин последните имат повече време да са разработват иновативни идеи с цел разрастване на вашия бизнес.

Сигурност

В наши дни сякаш всеки ден научаваме за нови и нови пробиви в сигурността, които засягат огромни корпорации като Target, Home Depot, Sony etc. Щом такива големи компании не са имунизирани срещу малуер, хакери и вируси, то може да си представите колко уязвим е вашия малък бизнес. И докато големите компании могат да си позволят да плащат глоби и да водят съдебни дела във връзка с такъв пробив в сигурността, подобни разходи са в състояние да изхвърлят от бизнеса един обикновен предприемач.

Голяма грешка е да предполагате, че сте защитен, само защото никой не би се занимавал да хакне данните, свързани с вашия бизнес. В действителност, тъй като малките предприятия обичайно са по-малко защитени от онлайн заплахи, точно те са предпочитани цели за атаки на онлайн хакерите. Професионалните доставчици на облачни услуги могат да ви помогнат с тези проблеми като ви предложат далеч по-високо ниво на сигурност в сравнение с това, което обичайно могат да осигурят собствениците на малки предприятия. В този смисъл съхраняването на данните ви на облак ви гарантира, че те са защитени от

експерти, чиято работа е да са в крак с последните налични заплахи за сигурността.

Непрекъснатост

Природни бедствия, кражба или инциденти могат да унищожат най-важните данни на едно предприятие, ако последните се съхраняват само на твърди дискове във вътрешните сървъри на офиса. В последните години екстремни климатични събития като наводнения, урагани и снежни бури изкараха извън строя много много малки компании — поне временно. Статистиката на FEMA показва, че между 40 и 60 процента от малките предприятия, които са засегнати от бедствия, никога повече не започват дейността си отново.

Чрез облачното съхраняване и услугите по архивиране могат периодично да се създават копия на вашите данни и приложения онлайн, за да може последните винаги да са в безопасност от природни бедствия и да могат да бъдат възстановени в случай на инцидент. Автоматичното архивиране на копия премахва риска от човешка грешка в процеса по създаването им, като по този начин значително повишава нивото на сигурност. В допълнение следва да посочим, че много от облачните разрешения за архивиране предлагат възможността да се запазват няколко версии на даден документ автоматично, за да можете по-лесно да имате достъп до по-старите версии на документа.

Мобилност

Работата от разстояние е предпочитан вариант за много от служителите тези дни. И, разбира се, собствениците на малки натоварени предприятия често прекарват нощите си в работа вкъщи. Когато използвате облачни услуги, няма нужда да си препращате имейли с файлове за по-късно преглеждане или да трябва да не забравите да донесете устройството си във вас. Вместо това, вие и вашият екип ще имате достъп до последните версии на документите и всичките си данни чрез Интернет връзка, независимо къде се намирате. Облачните услуги действително променят правилата на играта за продавачи и други предприемачи, които често пътуват по бизнес, за да посетят клиенти и да проучат определени възможности лично. С помощта на облачните услуги никога

повече няма да се тревожите дали сте запазили последната версия на презентацията, контакта или предложението си.

Ефективност

Облачно базираният софтуер се актуализира автоматично, без полагане на усилия от ваша страна. Благодарение на липсата на нужда от собствено поддържане на системите ви, вашите служители стават все по-ефективни. Работниците няма нужда просто да се размотават и да чакат (и да не работят) докато вашия IT специалист прави актуализации или оправя техните компютри. И тъй като те винаги имат последните версии на софтуера, техните компютри са в състояние да оптимизират максимално своето представяне. Наличието на по-малко бъгове и по-голяма скорост означава, че вашите служители ще могат да свършат много повече работа за значително по-малко време.

Свързаност

Облачните услуги предоставят нови начини за дистанционни или виртуално свързване със служители, потребители или контрагенти. В този смисъл вие можете да правите виртуални конферентни разговори или видео конференции онлайн чрез използването на облачна VoIP технология. Облачно базираните инструменти за сътрудничество позволяват на екипите да преглеждат, обсъждат и променят документи или презентации едновременно в (почти) реално време. Когато няма нужда да променяте физическото си местоположение, за да проведете среща, това постепенно увеличава възможностите ви за комуникация с потребителите, а това автоматично означава повече доволни клиенти и по-силна връзка с последните.

Достъпност

Спестяването на средства е една от най-големите ползи на облачните услуги за малките предприятия. Много доставчици на облачни услуги вече предлагат безплатни версии са услугите си, които често са достатъчни за нуждите на една малка компания. Вместо да трябва да правите единично плащане на значителна стойност, вие плащате за облачните услуги, които използвате на месечна или

абонаментна база. Тези модели за разпределение на плащанията ви помагат да генерирате паричен поток, тъй като разходите се разпределят във времето.

Използването на облачни услуги също така намалява вашите разходи за изплащане на заплати, защото доставчика на облачните услуги поема извършването на тези задачи, които обичайно се вършат от ИТ специалиста във всяка фирма. На последно място, но не и по значение, при използването на облачни услуги вие плащате само за това, което използвате. Това ви гарантира, че не харчите средства за хардуер, който не използвате например, или пък за софтуер, от който компанията ви няма нужда.

Възможност за разрастване

Облачните услуги са страхотен начин за малките предприятия да планират своето разрастване. С разрастването на вашата компания вие можете лесно да промените вида на използваните от вас облачни услуги, да добавите нови сървъри или потребители почти моментално. Няма нужда да купувате нов и скъпоструващ хардуер и софтуер, тъй като вие просто “наемате” всичко, което ви трябва от доставчика си на облачни услуги. Като допълнителна помощ за справяне с евентуалното ви разрастване, облачните услуги ви позволяват също така да се справите с неочакван и бърз растеж. Какво ще стане, ако продуктът ви изведнъж придобие популярност в социалните мрежи и вашият уебсайт се претовари с поръчки на посетители?

В такъв случай вие можете бързо да решите проблема, повишавайки нивото си на облачно базирани услуги или добавяйки нови облачно базирани инструменти. Облачните услуги могат да ви помогнат също така и с неочаквани или сезонни забавяния. Ако пък дейността ви се понижи, спирате предлагането на продукт или услуга, или пък освобождавате част от персонала, просто можете да понижите нивото на облачните услуги, които използвате. По този начин, чрез осигуряването на достъпна възможност за разрастване, облачните услуги позволяват на малките предприятия да обърнат нещата в своя полза.

[Business.qld.gov.au. (2018). *Cloud computing for business | Business Queensland*. [online] Available at: https://www.business.qld.gov.au/running-business/it/cloud-computing]

Присъединете се към тълпата в облака

Без съмнение изчислителните облаци предлагат редица предимства за собствениците на малки предприятия. Може би най-голямото предимство се състои в това, че използването на облачни услуги ви позволява да се фокусирате по-малко върху техническите си проблеми и повече върху същинската дейност на предприятието си. Благодарение на гъвкавостта и простотата при използване на облачните услуги, вие можете бързо да се възползвате от възможностите им и да разраснете бизнеса си до пълния му потенциал.

[Business.qld.gov.au. (2018). *Cloud computing for business | Business Queensland*. [online] Available at: https://www.business.qld.gov.au/running-business/it/cloud-computing]

Безопасност на облака и данните

Поддържането на безопасността на облака се отнася до намирането на правилните доставчици и прилагането на технология, която използва едновременно идентификация на самоличност и криптиране на данните. Ето 10 въпроса във връзка със сигурността, които да попитате вашите потенциални доставчици на облачни услуги, преди да решите да подпишете договор за използване на услугите им:

- Кой може да вижда информацията ми?
- Данните ми в няколко центрове за данни на различни места ли се държат и защитени ли са те от регионални атаки?
- Какви мерки за защита на данните ми използвате?
- Какви специфични мерки за криптиране на данните ми използвате?
- Как управлявате криптиращите си ключове?
- Как следва да възстановите данните ми, ако последните са загубени вследствие на сриване на сървъра или кибератака?
- Какви сертификати за сигурност притежавате?
- В съответствие ли сте с най-съвременните протоколи за сигурност?
- Какво може да се обърка при въвеждането на услугите?
- Дистрибутор ли е и ако да – кой отговаря за услугата и поддръжката?

C. Използване на големи масиви от данни (big data) – възможности и заплахи

Big Data: Какво представляват и защо са важни

Изображение 8: Big Data приложение

Big data е термин, който описва голямо количество данни – структурирани или неструктурирани – които заливат бизнеса ежедневно. Важно е да се подчертае, че не количеството данни са от значение, а какво организациите правят с тези данни. Big data могат да бъдат вътрешно анализирани с цел оптимизирането на решения и стратегически бизнес действия.

При дефинирането на big data е важно да разберем съвкупността от неструктурирани и мулти-структурирани данни, които са включени в обема от информация.

Неструктурираните данни представляват такава информация, която не е организирана или не се интерпретира лесно от обикновените бази данни или

модели на данни, като в общия случай те съдържат много текст. Метаданни, Twitter туитове и публикациите в други социални мрежи са добър пример за неструктурирани данни.

Мулти-структурираните данни се отнасят до разнообразни формати и видове данни, които могат да бъдат извлечени от взаимодействията между хора и машини, като например уеб приложения или социални мрежи. Добър пример за тези данни са log данните, които включват в себе си комбинация от текст и визуални изображения със структурирани данни като форма или информация за транзакции. Докато дигиталните смущения трансформират комуникационните канали и тези за взаимодействие — и докато търговците повишават нивото на потребителско преживяване чрез устройства, уеб настройки, комуникация лице в лице и социални платформи — мулти-структурираните данни ще продължават да се подобряват.

[Forbes.com. (2018). [online] Available at: https://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data]

Защо големите масиви от данни (Big Data) са важни?

Важността на big data не произтича от факта какво количество данни притежавате, а какво правите с наличните данни. Можете да получите данни, от който и да е източник, които да анализирате и да получите отговори, които ще ви позволят:

1. Намаляване на разходите
2. Спестяване на време
3. Разработване на нови продукти и оптимизиране на предлаганите услуги
4. Вземане на умни решения.

Когато комбинирате big data с висококачествени анализи, вие можете да постигнете свързани с бизнеса задачи като:

- Определяне на основните причини за технически проблеми и дефекти в почти реално време.

- Генериране на купони към момента на продажбата, базирани на навиците на купувача при купуване.
- Преизчисляване на цели рискови портфолиа за минути.
- Засичане на измамно поведение, преди да е навредило на организация.

Какви са ползите за бизнеса от големите масиви от данни (big data)?

Фигура 9: Ползи за бизнеса от използването на големи масиви от данни

- Използването на big data намалява разходите

Скорошна статия на Tech Cocktail разглежда как туристическата агенция Twiddy & Company Realtors намалява своите разходи с 15%. Компанията сравнява таксите за поддръжка на своите изпълнители в сравнение със средните такси на

други доставчици. Благодарение на този процес компанията установява и елиминира грешките при обработване на фактури съставянето на автоматизирани графици за поддръжка.

- Използването на big data увеличава вашата ефективност

Използването на дигитални технологични инструменти значително повишава нивото на ефективност на вашето предприятие. Чрез използването на такива инструменти като Google Maps, Google Earth и социални медии вие можете да извършвате много задачи от бюрото си, без да имате допълнителни пътни разходи и като си спестявате доста време. Тези инструменти спестяват и доста време.

- Използването на big data подобрява вашето ценообразуване

Използването на инструмент за икономически анализ може да ви помогне да направите оценка на финансите си, което от своя страна ще ви даде по-ясна представа какво е състоянието на вашето предприятие.

- Можете да се конкурирате с големите предприятия

Използването на същите инструменти, които използват големите предприятия ви позволява да бъдете конкурентни на последните, тъй като вашето предприятие увеличава продуктивността си, благодарение на използването на такива инструменти.

- Позволява ви да се фокусирате върху регионалните предпочитания

Малките предприятия следва да се фокусират върху регионалната среда, в която извършват своята дейност. В този смисъл big data ви позволява да прегледате по-подробно харесванията и предпочитанията на вашите клиенти. Щом веднъж вече познавате предпочитанията на клиентите си и показвате лично отношение спрямо тях, това ви дава предимство пред конкуренцията.

- Използването на big data за увеличаване на продажбите и лоялността на вашите клиенти

Дигиталните следи, които оставяме след себе си ни дават възможност да установим нашите предпочитания при покупки, вярвания и др. Тези данни позволяват на предприятията да предлагат своите продукти и услуги точно на хората, които са заинтересовани от тяхната покупка. Дигитални следи се оставят, когато потребителите ви сърфират онлайн и публикуват неща в социалните мрежи.

- Използването на big data ви гарантира, че наемате правилните за вас служители

Компаниите за наемане на служители могат да анализират достъпната информацията за един кандидат и неговите профили в социални мрежи (LinkedIn и други), като чрез използването на определени ключови думи може да се провери дали кандидатът отговаря на нужната характеристика. Процесът по наемане на служители вече не включва само хартиените документи на служителя и тяхното представяне на интервюто, което се дължи основно на big data.

[King, A. (2018). *7 Benefits to Using Big Data for Small Businesses - IndustriusCFO*. [online] IndustriusCFO. Available at: http://www.industriuscfo.com/7-benefits-using-big-data/]

D. Подобряване на дигиталните умения на служителите

Проблеми в областта на бизнес дигитализацията и дигиталните умения

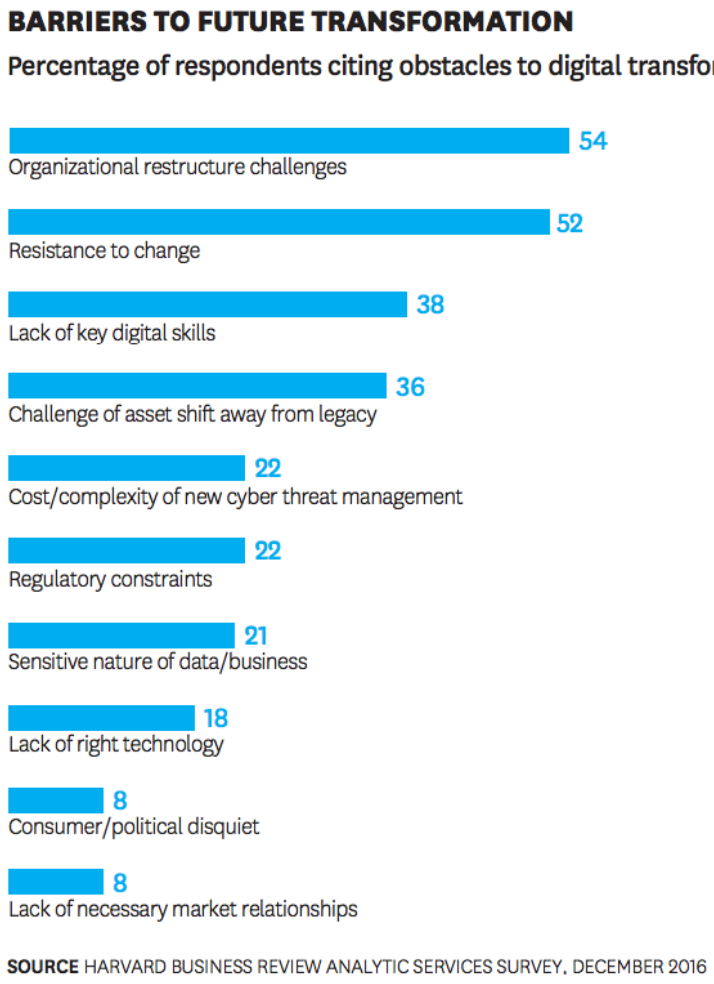
Дигиталната трансформация е в състояние да промени всеки един аспект от бизнес пейзажа, стига началниците и собствениците на предприятия да са готови да приемат тази промяна. Въпросът е какво е състоянието на смущенията в дигиталните услуги и какво трябва да очакват предприятията?

Всъщност ние вече се намираме в период на дигитална трансформация, който период води до различни ползи за предприятията. Въпросът е какво можем да

очакваме през следващите няколко години и как предприятията могат да останат в крак с ежедневните промени, които се отразяват на тяхната дейност?

Harvard Business Review Analytics Services и Microsoft публикуваха доклад, наречен “Конкуренцията през 2020: победители и губещи в условията на дигитална икономика“, в който правят общ преглед на състоянието на дигиталните смущения и изследват начина, по който началниците на предприятия реагират на тези смущения. Една от най-достойните за отбелязване точки в това изследване се състои в опита да се изведе връзка между проблемите на бизнес дигитализацията и дигиталните умения.

Дигиталната трансформация не може да се постигне без преодоляването на определени предизвикателства, като много проблеми възникват в процеса по нейното интегриране в едно предприятие. Анкетираните в това проучване били помолени да посочат най-значимите бариери пред осъществяването на дигитална информация през следващите няколко години, а 54% процента от тях посочили организационната структура на своите предприятия като най-големия проблем в осъществяването на процеса по дигитализация.

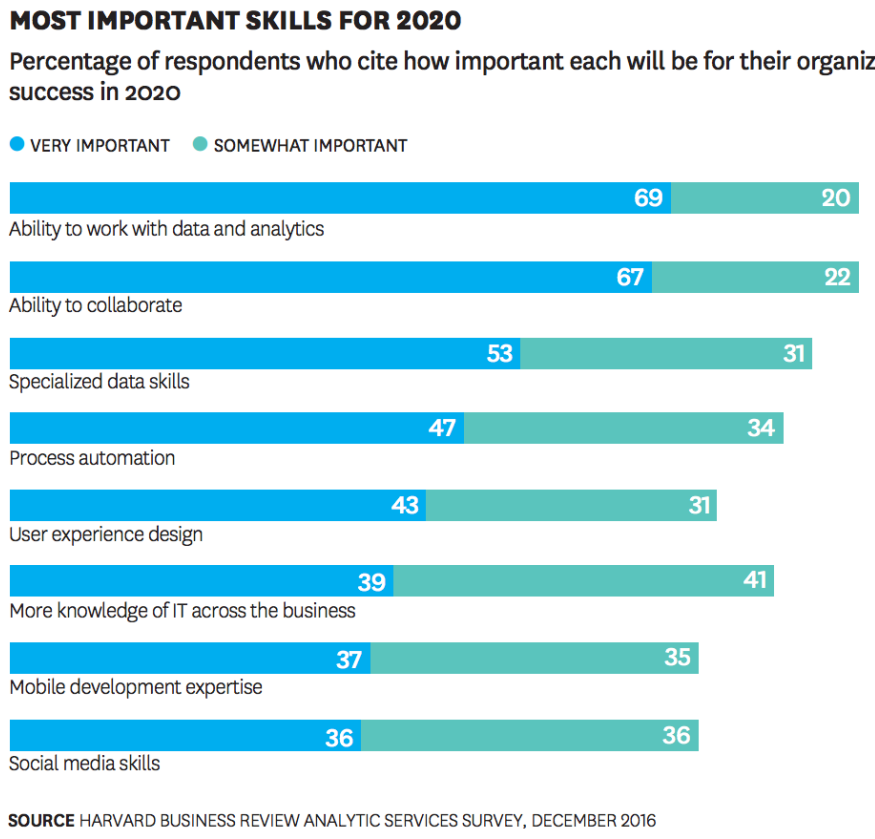


Фигура 10: Проблеми при бъдеща трансформация

Подобен процент от анкетираните (52%) са посочили нежеланието за промяна като ключов проблем пред дигиталната трансформация на своите предприятия, а други отговори на въпроса включват липсата на дигитални умения, ресурси и бюджет като пречка за извършването на такава трансформация. Нежеланието за промяна е може би най-интересното установено предизвикателство пред приемачите, тъй като показва, че някои организации не са особено възприемчиви към новите тенденции. Поради това е възможно да се наложи извършването на последващи обучения, за да могат предприемачите да осъзнаят ползите от дигитализирането на своите предприятия.

Нещо повече, липсата на ресурси, бюджет и умения не могат да бъдат пренебрегнати, тъй като последните пораждат нуждата за всички. Според анкетираните най-важното умение, което дигиталните лидери трябва да

притежават през 2020 година, е способността да работят с данни и да анализират последните, като се фокусират върху специализираните умения за работа с данни, които се нареждат на трето място в списъка. Способността за сътрудничество се нарежда на второ място сред най-необходимите умения, като анкетираните ясно са определили нуждата повече хора в тяхната организация да развият такива умения, които са необходими за осъществяването на дигитална трансформация в предприятието.



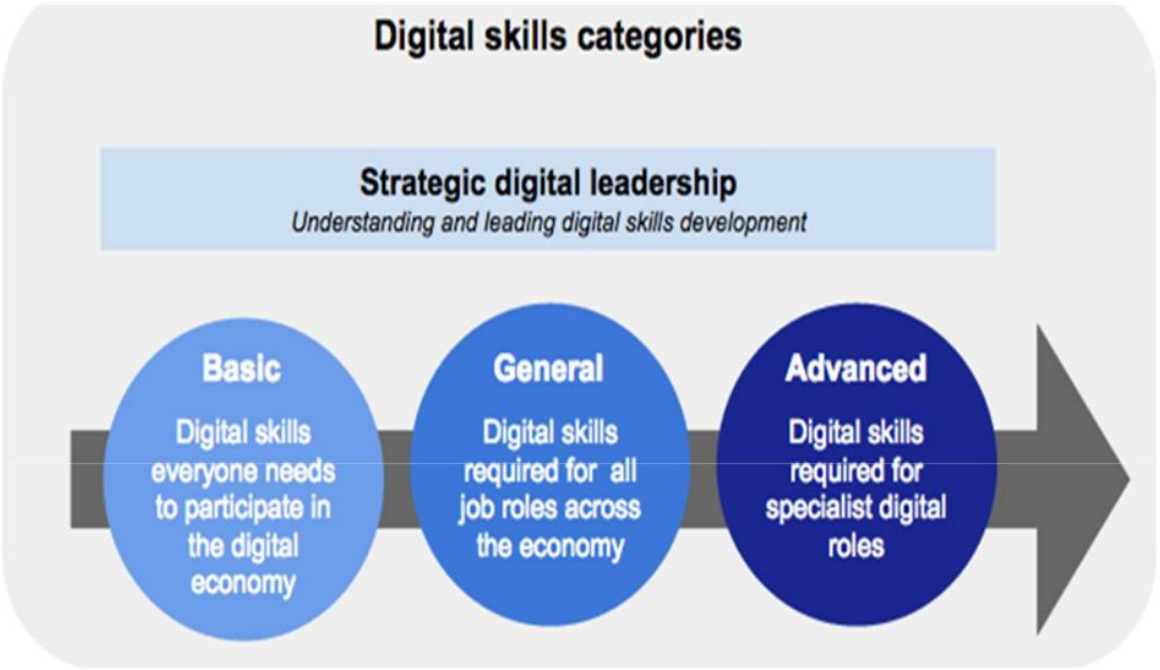
Изображение 11: Най-важните умения през 2020 г.

[The rising opportunity of digital transformation: What businesses need to know - ClickZ. [online]. Available at: https://www.clickz.com/the-rising-opportunity-of-digital-transformation-what-businesses-need-to-know/110987/]

Какво са дигиталните умения?

Дигиталните умения намират своите корени в сложната съвкупност от няколко ключови концепции за развитие на дигиталните умения, наречени ИТ грамотност, ИКТ грамотност, дигитална грамотност, дигитална компетентност, ИКТ плавност, компютърна грамотност, ИКТ умения, електронни умения, технологична грамотност, медийна грамотност, информационна грамотност, електронна грамотност, основни умения, умения на 21 век, мулти-грамотност и нови знания. Бляскавостта на термина дигитална грамотност произтича от неговото широко използване, като той се дефинира като: възможност за разбиране и използване на информация в множество формати и от широк кръг от източници, когато последната се представя чрез компютри.

Дигиталните умения включват знанието и възможността да се определи и извлече необходимата информация от дигиталните технологични източници, както и правилното използване на дигитални инструменти и съоръжения с цел въвеждане, достъп, организиране, интегриране и оценка на дигитални ресурси, както и изграждането на нови знания, създаването на медийни изрази и комуникация с други лица. Важно е да подчертаем, че дигиталните умения включват както технически умения, които са свързани с познаването и използването на дигитални системи, инструменти и приложения, така и умения за обработване на информация, които са когнитивните основи на дигиталната компетентност и ефективност.



s

Изображение 12: Категории дигитални умения

Защо вашата организация се нуждае от обучения, във връзка с дигиталните умения

Дигитализацията представлява трансформация. Потребителите вече могат да използват търсачки и социални медии на всеки етап от тяхното потребителско преживяване – 81% от тях посочват, че извършват онлайн търсене преди да направят покупка, а 70% от решението на купувача е взето още преди той да стигне до представителя на продавача на стоката. Дигиталните възможности вече позволяват на потребителите да се самообучават и да бъдат много по-внимателни, когато вземат своето окончателно решение за покупка на определен продукт.

Това създава задължение за различните организации да се запознаят и адаптират бързо към дигиталния растеж, ако искат да постигнат дълготраен успех сред клиентите и бизнесът им да бъде възможно най-доходоносен. 76% от маркетинг експертите смятат, че маркетингът се е променил повече в последните две години, отколкото в последните петдесет, което означава, че постоянното усъвършенстване на уменията е от ключово значение за успеха.

Организациите, които решат да привличат клиенти и перспективи чрез добре обмислена маркетингова стратегия, ще намерят за по-лесно изграждането на име на своята марка, генерирането на икономии на разходите и в последна сметка стимулиране на приходите. Поради тази причина обучените дигитални професионалисти се считат за незаменим актив за едно предприятие.

Въпреки неоспоримите ползи, които носи дигитализацията на едно предприятие, все още широк кръг от организации настойчиво отказват да започнат използването на дигитални инструменти и технологии. Независимо дали причината за това е в липсата на разполагаем бюджет и ресурси, страх от загуба на контрол или генерален скептицизъм, че дигитализацията може да доведе до значителна възвръщаемост на инвестициите, тези бариери срещу въвеждането на дигитални мерки следва да се преодолеят, за да се гарантира продължаващият и бъдещ организационен успех.

Отговорът на тези опасения е много прост. Една краткотрайна инвестиция в обучения по дигитални умения ще доведе до дълготрайна награда – ще се даде възможност на съответната организация и нейните служители да поддържат своето предимство пред конкуренцията и да са сигурни, че няма да изостанат в развитието си.

Ако все още се съмнявате, че организацията ви ще има ползи от прилагането на един стратегически план за устойчиво дигитално образование, погледнете някои от ключовите предимства по-долу:

1. Дигиталните умения са в състояние да мотивират вашите служители

Към настоящия момент е налице безпрецедентен недостиг на служители с дигитални умения в глобален мащаб, който недостиг се наблюдава във всички отрасли. В резултат на това, наемането на компетентни кандидати представлява трудност за всички организации, независимо от размерите им.

И тъй като тези организации се състезават помежду си да наемат малкото дигитално образовани професионалисти на пазара на труда, малките бизнеси страдат от това, поради невъзможността им да се конкурират с увеличаващите се високи заплати и други социални придобивки, които някои от корпорациите предлагат на служителите си.

Въпреки горепосочените обстоятелства, за съжаление нивото на дигитални умения в световен мащаб е стратегическо ниско. В доклада за изследване на дигиталните умения за 2016 година, маркетолози от Ирландия, Великобритания и САЩ тестват своята дигитална компетентност, като средният им резултат е само 38%. Тези резултати са в съответствие с широко разпространеното виждане, че те следва да подобрят своите дигитални маркетингови умения, за да продължат да са компетентни на своите позиции (86% Ирландия, 69% Великобритания и САЩ).

Все повече и повече компаниите проявяват интерес да наемат вече обучени международни специалисти като решение на проблема с недостига на талантливи кадри. Независимо от това, безсъмнено по-лесната и по-малко струващата възможност остава самостоятелното обучаване на талантливи кадри в компанията.

Adobe организациите, които имат план за своето дигитално израстване, целят да обучат и развият уменията на своята съществуваща работна сила. Това е така, защото те осъзнават, че възможността за професионално и личностно развитие често се явява основен приоритет за служителите, като последните могат да се почувстват разочаровани и недостатъчно стимулирани, ако в компанията не съществува такава възможност.

Ако организациите решат да обучат своите служители в областта на дигиталните технологии, те не само ще имат полза от новите им способности и стимулирано отношение към работата, но и ще могат да използват обученията им като метод за задържането на служителите си.

2. Дигиталните умения могат да помогнат за увеличаване на приходите ви

Дигиталните инструменти и технологии вече имат дълбоко въздействие върху световната икономика. През 2016 година, за пръв път приходите от онлайн реклама надминаха приходите от телевизионна реклама, като прогнозираните приходи от дигитална реклама се оценяват на 260 милиарда долара до 2020 г.

Разходите за дигитални реклами и бюджетите за маркетинг систематично се увеличават, тъй като все повече организации започват да осъзнават предимствата, които дигитализацията носи на бизнеса им. Според доклад на

Capgemini, компаниите с по-голям дигитален производствен интензитет извличат повече от техните физически активи и са с между 9 и 26% по-печеливши от останалите.

Съществуват твърде много технологични предимства, които организациите могат да използват за разрастването си, за да използват само традиционен маркетинг и обичайни подходи за продажба на стоките си. Само 28% от потенциалните клиенти, на които се обадите, имат желание да проведете разговор, а само 1% от тези обаждания се превръщат в определени уговорки. С увеличаване на дигиталните възможности на потребителите, те разчитат все по-малко на опита на търговски представители и все повече на своите собствени възможности на проучат пазара. В отговор на тази промяна в силите, организациите трябва да съживят своите продажби и функциите на маркетинговите си отдели, както и да синхронизират използването на канали и платформи с тези, които потребителите използват, за да достигнат ефективно последните.

Дигиталните умения могат да позволят вашата организация да установи по-добри връзки със своите потребители, да се утвърди като лидер в съответната индустрия и да увеличи броя на клиентите си. Обученията за придобиване на дигитални умения несъмнено ще доведат до тези резултати.

3. *Дигиталните умения могат да доведат до спестяване на значителни разходи*

Всички сме чували фразата “за да изкараш пари, трябва да инвестираш пари”. Но може ли едновременно да харчим и да спестяваме пари? С помощта на пълен пакет от цифрови умения, организацията ви може да постигне и двете.

Американската асоциация за обучение и развитие (ASTD) събра информация за обучения от над 2500 фирми и заключи, че организациите, които предлагат цялостно обучение имат 218% по висок приход на един служител в сравнение с тези организации, които не предлагат цялостни обучения. Това означава, че простото мотивиране на служители чрез предоставянето им на обучения може да спести значително финансови средства на организациите. Нещо повече, според Американската асоциация по мениджмънт разходите за наемане и

обучение на нов служител са между 25 и 200% от годишната компенсация, така че провеждането на обучения може да ви спести разходите по ненужно наемане на служители. В допълнение към гореизложеното можем да посочим, че други финансови ползи могат да включват икономии на труда, намаляване на работните дни и същевременно увеличаване на производителността.

Основните принципи на дигиталния маркетинг са базирани на работната ефективност и ефективността на разходите:

- Настройките за прецизно насочване на рекламите могат да доведат до по нисък разход на продажбите или услугите
- Лесната и незабавна връзка с определена целева аудитория може да доведе до провеждането на повече разговори на по-малка цена
- Изобилието от данни, предоставени от инструменти за анализиране, дават безценен вътрешен поглед върху нещата, който може да ви помогне при определянето на дигитална стратегия и избягването на ненужни разходи.

Според компанията Gartner 40% процента от организациите твърдят, че значително са повишили спестените си разходи чрез използването на методи за дигитален маркетинг при рекламирането на своите продукти и услуги. Тези спестявания могат да бъдат съответно реинвестирани във въвеждането на още дигитални маркетингови техники и тактики, чрез които да се постигне същият или по-голям приход при по-нисък генериран разход за организацията.

4. *Дигиталните умения могат да помогнат на вашата организация да развие своята конкурентноспособност*

Добрият комплект от дигитални умения вече не представлява лукс за организациите – той е основополагащ елемент на всеки конкурентен бизнес модел. Въпреки това в нашия последен доклад относно дигитални умения се посочва, че все още много организации остават неангажирани по отношение на дигиталните умения на служителите си. Само 31% от организациите в САЩ, 25% от тези във Великобритания и 40% от тези в Ирландия смятат, че са дигитално ангажирани, като преобладаващото мнение сред служителите е, че темповете на технологични и дигитални промени са твърде бавни.

Според проучване на McKinley пък 90% от всички маркетингови позиции изискват наличие на дигитални умения. Това е така, тъй като дигиталните специализации са далеч по-търсени, ефективни и измерими в сравнение с традиционните техники. В този смисъл дигитализирането е задвижваният от данни ключ към успеха на една организация. То може да доведе до рационализиране на процесите и да доведе до разширяване на възможностите на организацията ви. Възможността за получаване на точна вътрешна информация и привеждането ѝ в действие означава, че ако бъдат приложени успешно дигиталните инструменти и канали, могат да помогнат на различните организации да се развият и същевременно да поддържат високо ниво на конкурентност.

Социалните медии могат да осигурят платформа за обслужване на онлайн потребители, което ще подобри задържането на вашите клиенти. Мобилният маркетинг може да помогне на една организация да развие всестранното присъствие на марката си. Имейл маркетингът от своя страна може да спомогне за изграждането на ценна връзка с потребителите чрез изпращането на полезно съдържание на всеки етап от клиентското им преживяване. Друг полезен съвет е, че всяка кампания, която разработвате може да бъде измерена и оптимизирана с помощта на инструменти за анализиране.

Някои от основните пречки при въвеждането на дигитализацията са липсата на вътрешни експерти с опит, както и липсата на организационно желание за осъществяването ѝ. За да осъзнаете в цялост как дигитализирането на бизнеса ви може да помогне на вашата организация, оказва се от ключово значение да провеждате обучения за придобиване на такива умения, като само така ще можете да разберете огромните ползи от това и да предприемете действия.

[Digital Marketing Institute. (2018).*Why your organization needs digital skills training*. [online] Available at: https://digitalmarketinginstitute.com/blog/why-your-organization-needs-digital-skills-training]

Е. Контролен списък за дигитализация на бизнеса

Готови ли сте за дигиталната ера?

Много от собствениците на малки предприятия вярват, че вече използват дигитални технологии ефективно, само защото имат уебсайт или страница във Фейсбук. Истината е, че съществуват много други начини за използване на дигиталните технологии с цел подобряване на вашите бизнес резултати.

Провеждането на дигитален одит ще помогне да разберете дали вашият бизнес е дигитален новак, дигитално активен или дигитално напреднал.

Дигитализация: Контролен списък от 10 стъпки за начало

Пътят до пълната дигитализация е дълъг. За да сте сигурни, че няма да се изгубите, трябва да започнете със следните стъпки:

	✓
Съберете екипа си Подчертайте големите ползи, които дигитализацията ще донесе не само на компанията ви, но и на всички ваши работници. Нарисувайте им картина, който ще развълнува всички. Ако вие сте изпълнителният директор, постарайте се всички да видят, че приветствате тази промяна.	
Изберете своята цел Представете си всички осезаеми ползи, които дигитализацията ще донесе на вашия бизнес, компания и общност. Решете какво искате да постигнете чрез дигитализацията и се придържайте към целта си.	
Разберете бъдещите си потребители	

Дръжте под око потребителите си, които са родени през настоящия век, защото ежедневното използване на технологии е в тяхната природа. Разработете технологични решения, за да посрещнете нуждите на вашите бъдещи клиенти и да поддържате вашата бъдеща конкурентноспособност.	
Начертайте карта на дигиталното преживяване Разучете начина, по който вашите настоящи целеви потребители използват дигитални платформи. Това ще ви помогне да установите правилните дигитални решения, които ще са ви нужни, за да достигнете до тях.	
Създайте дигитална работна група Въвлечете всички ваши служители, като създадете работна група за дигитални шампиони. Това ще ви помогне да се запознаете и с други области в бизнеса. Работната група може да си сътрудничи относно времето за доставка, поддържане на графиците на проектите и поддържане на осведомеността на техните екипи.	
Инвестирайте в правилните инструменти Потърсете подходящ, специфичен за вашата индустрия софтуер и ИТ инструменти за вашето дигитално предприятие. От счетоводство, управление на инвентара, търговски обекти, заплати и други – съществуват буквално стотици приложения, които могат да помогнат на вашия бизнес. Те включват и софтуер за защита на данните, мобилен достъп, докладване в реално време и интеграция, като целта им е да помогнат за плавен и безпроблемен преход.	
Възползвайте се от SaaS платформата	

Използвайте правилната SaaS (Софтуер като решение) платформа с цел по-добро използване и управление на вашите важни бизнес данни. SaaS инструментите, които си комуникират помежду си на една платформа могат да елиминират външното въвеждане на данни, а това означава повече свободно време, за да ръководите предприятието си. SaaS доставчиците също така имат най-високо ниво на сигурност, така че да сте сигурни, че цялата ви информация е в сигурни ръце.	
Намалете разходите си Демонстрирайте дръзко лидерството си, като вземате трудни решения. Знайте какво можете и какво не можете да направите, и по-важното – мястото на нещата в рамките на стратегията за дигитална трансформация. Ако това изисква да се откажете от правенето не необосновани инвестиции в стари системи и софтуер – поемете риска.	
Измервайте резултатите си Следете как вашите дигитални инициативи приемат цифрови изражения. Сравнете ги с вашите първоначални цели и преценете дали подходът ви помага за постигане на възможно най-добри резултати.	
Споделяйте вашите нови знания Обучете вашия екип, за да сте сигурни, че вашите служители имат умения, знания и опит, за да изпълнят максимално вашата дигитална стратегия.	

F. Терминологичен речник

Big data (големи масиви от данни) - Big data са данни, които са толкова обемни и сложно конструирани, че традиционните софтуери за обработка на данни не могат да се справят с обработването им. Предизвикателствата при Big data включват обобщаване, съхраняване и анализиране на данни, търсене, споделяне, трансфер, визуализация, заявяване, обновяване, информационна защита и източници на данни.

Изчислителни облаци – Изчислителните облаци са парадигмата на информационните технологии (ИТ), която дава възможност за всеобщ достъп до споделени „басейни“ от конфигурируеми системни ресурси и услуги на високо ниво, които могат да бъдат обезпечени с минимални управленски усилия, често дори през Интернет. Изчислителните облаци разчитат на споделянето на ресурси за постигането на последователност и икономии от мащаба, подобни на тези при обществените услуги.

Дигитален бизнес – Дигиталният бизнес е създаването на нови бизнес дизайни чрез размиването между дигиталния и физическия свят.

Digital Disruption - цифровото смущение е ефект, който променя основните очаквания и поведения в културата, на пазара, в промишлеността или в процесите, причинен от или изразен чрез цифрови възможности, канали или активи.

Дигитални умения – Всички умения, които са свързани с това човек да бъде дигитално грамотен.

Дигитализация – Дигитализация е използването на дигитални технологии с цел промяна на бизнес модел и осигуряване на нови източници на приходи и нови възможности за производство; това е процесът по преобразуването на един бизнес в дигитален такъв.

Машинно обучение – алгоритмите за машинно обучение са съставени от много технологии (учене в дълбочина, невронни мрежи и обработка на естествен език), използвани в самостоятелно и контролирано обучение, които действат, ръководени чрез уроци от съществуваща информация.

Платформа (Дигитален бизнес) – платформата е продукт, който служи или подпомага действието на други продукти или услуги. Платформи (в контекста на дигиталния бизнес) съществуват на много нива. Те варират от платформи на високо ниво, които задействат платформата на бизнес модела, до платформи на ниско ниво, които осигуряват събиране на бизнес и/или технологични възможности, които други продукти или услуги употребяват, за да доставят своите бизнес възможности. Платформите, които задействат платформите на бизнес моделите, имат свързани бизнес екосистеми.

G. Заключения и допълнителни източници

Без съмнения, дигиталната трансформация ще промени облика на редица индустрии. Това е следващата стъпка от индустриалната революция. Бизнес дигитализацията, всъщност не е пълна дигитална трансформация на бизнеса и все пак е ключова стъпка в тази посока.

Независимо от нарастващото значение на бизнес дигитализацията, това е път, който изобщо не е лесен за изминаване. Над половината от висшите ръководни кадри на организациите в Европа смятат, че дигиталните иновации не са постигнали очакваното голямо влияние по отношение на дейността на техните организации. Често тези корпорации вярват, че дигитализацията е едно тепърва прохождащо направление и не са наясно какво точно представлява тя и какво могат да очакват.

Определено е предизвикателство за различните организации да са в крак с множеството нови дигитални технологии като изкуствен интелект, използване на биометрични данни, изчисления с квантови компютри, роботика и други. Въпреки това, когато компаниите поставят потребителя в центъра на тези дигитални иновации и използват дигиталните технологии, за да създадат впечатляващи преживявания за тях, ние виждаме и се потвърждава отново и отново фактът, че в тези случаи ефектът е наистина голям. Фирмите често разбират “дигиталното” като проект, но тази настройка не може да доведе до голям ефект върху техния бизнес.

Дигиталните технологии коренно променят начина, по който компаниите се представят на пазара и тяхната вътрешна организация. За да може дигиталните технологии да осигурят голямо въздействие, цялата организация трябва да е в съответствие с тях и да промени начина си на функциониране.

Компаниите, които вярват, че интегрирането на нови технологии върху вече изградена инфраструктура е ключовото предизвикателство пред тях по отношение на дигиталните иновации, просто започват промяната по грешен начин. Дигиталните технологии не са тук, за да поправят нещо, което не работи. Дигиталните технологии позволяват на компаниите из основи да преосмислят по какъв начин следва да предлагат продуктите си на пазара.

Поддържането на целия екип, хората зад бизнеса, които са привлечени от тази промяна, също е от решаващо значение. Служителите трябва да притежават определени умения, които ще им помогнат да възприемат промяната и да работят ефективно в новата дигитална среда.

Изглежда все пак, че хората са най-значимият фактор за успешното интегриране на новите технологии в бизнес средата – те са инструментът, който води един или друг бизнес до успех.

Допълнителна информация:

За да постигнете дигитална трансформация, вие трябва напълно да познавате действието на машинното обучение и изкуствения интелект. Трябва също така да сте наясно с Блокчейн революцията и как технологията, стояща зад Биткойн променя значението на парите и бизнеса, защото рано или късно всяка организация ще има нужда да разбере и да използва Блокчейн под някаква форма. Възможността да изберете правилния екип, да ги обедините, заедно около една цел и да ги мотивирате да постигнат повече, отколкото са си представяли, това също е умение, върху което ще трябва да поработите. Вече видяхте как Big Data промени света на информационните технологии и света на бизнеса. Истината е, че в много аспекти тази технология тепърва започва своето развитие. Много лидери все още не разбират или не приемат силата на вземането на решенията след анализ на данни, без значение значими ли са решенията. Разберете възможностите, които Big data отваря, както и заплахите

зад тях. Можете също така да изучавате начина, по който стартиращите предприятия работят и как те използват непрестанно иновации, за да създадат успешен бизнес. Има причина, че стартиращите предприятия толкова често нарушават по-големи, по-утвърдени организации - и това е то. Прилагането на принципите на опростеност и гъвкавост във вашата собствена организация ще ви помогне да се адаптирате към бързо променящия се пазар и да бъдете по-малко уязвими.

Н. Източници

1.i-scoop: Digitization, digitalization and digital transformation: the differences

(https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption)

2.Gartner Executive Programs: Taming the Digital Dragon: The 2014 CIO Agenda

3.i-scoop: Digital business: transformation, disruption, optimization, integration and humanization

(https://www.i-scoop.eu/digital-business)

4.tieto: How Digitalization is Changing the Face of Business

(https://perspectives.tieto.com/blog/2015/07/how-digitalization-is-changing-the-face-of-business)

5. Forbes: Digital Business is Everyone's Business

(https://www.forbes.com/sites/gartnergroup/2014/05/07/digital-business-is-everyones-business/#7f60b8b67f82)

6. cio: Digital transformation: Why it's important to your organization

(https://www.cio.com/article/3063620/it-strategy/digital-transformation-why-its-important-to-your-organization.html)

7.insightsuccess: Role of Digitization in Today’s Business World

(https://www.insightssuccess.com/role-of-digitization-in-todays-business-world)

8.Forbes: Digital Transformation And Innovation In Today's Business World

(https://www.forbes.com/sites/brianrashid/2017/06/13/digital-transformation-and-innovation-in-todays-business-world/#341a36e74905)

9.McKinsey & Company: Raising your Digital Quotient

(https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/raising-your-digital-quotient)

10. Deloitte: Doing business in the digital age: the impact of new ICT developments in the global business landscape (April 2013)

11.Gartner: The New Risks of Digital Business

(https://www.gartner.com/smarterwithgartner/the-new-risks-of-digital-business)

12.i-scoop: Cybersecurity: security risks and solutions in the digital transformation age (https://www.i-scoop.eu/cyber-security-cyber-risks-dx)

13.wired: 5 cloud business benefits (https://www.wired.com/insights/2012/10/5-cloud-business-benefits)

14. dreamhost: What is Cloud Computing and How Can It Help Your Small Business? (https://www.dreamhost.com/blog/cloud-computing-for-business)

15.McKinsey & Company: How companies are using big data and analytics (https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/how-companies-are-using-big-data-and-analytics)

16. Business News Daily: 8 Big Data Solutions for Small Businesses (https://www.businessnewsdaily.com/6358-big-data-solutions.html)

17.sas: How Midsized Businesses Can Take Advantage of Big Data (white paper)

18.Bernard Marr & Co: How Is Big Data Used In Practice? 10 Use Cases Everyone Must Read (https://www.bernardmarr.com/default.asp?contentID=1076)

19. Digital Skills Academy: The Top 10 Digital Skills Tech Companies are Looking for Today (https://digitalskillsacademy.com/blog/the-top-10-digital-skills-tech-companies-are-looking-for-today)

20.Skillsoft: What are digital skills? A comprehensive definition for modern organisations (white paper)

21.Digital Marketing Institute: Why your organization needs digital skills training (https://digitalmarketinginstitute.com/blog/why-your-organization-needs-digital-skills-training)

22.Department for Culture, Media and Sports, France: Digital Skills for the Digital Economy

23. Smallbizdaily.com: The Benefits of Being a Digital Business (https://www.smallbizdaily.com/benefits-digital-business/)
24. Forrester: Why Do Digital Business Transformations Fail? (https://go.forrester.com/blogs/15-04-01-why_do_digital_business_transformations_fail/)
25. Business Queensland: Cloud computing for business (https://www.business.qld.gov.au/running-business/it/cloud-computing)
26. Business News Daily: Cloud Computing: A Small Business Guide (https://www.businessnewsdaily.com/4427-cloud-computing-small-business.html)

ЧАСТ II

Дигитална Сигурност за Млади Социални Иноватори

Списък с абревиатури

Абревиатура	Определение
SBI	Инициатива за социално предприемачество
SME	Малки и средни предприятия
IoT	Интернет на нещата
SEO	Оптимизиране на търсещи системи
IT	Информационни Технологии

A. Въведение

Настоящата глава цели да предостави на социалните предприятия и социалните иноватори по-задълбочен поглед върху концепцията на социалното предприемачество в условията на дигиталната ера, както и върху начина, по който работната среда се променя от традиционната офис среда към дигитална работна среда в областта на „Интернет на нещата“ (Internet of Things). В главата се подчертават потенциалните възможности и заплахи за социалното предприемачество, извършвано в онлайн среда, като се дават и предложения за правилното му осъществяване в тази среда с цел избягването на възможни неблагоприятни последици. На последно място, в настоящата глава се посочват и някои полезни съвети за социалните иноватори и предприемачи, както и е съставен контролен списък, който да улесни последните при прилагането на мерките за осигуряване на дигиталната сигурност в техните социални предприятия.

“Едно предприятие може да бъде социално, само когато изпълнението на социалните цели, е основна задача на неговата дейност. [11] “

B. Социално Предприемачество в Дигиталната Ера

Повече от очевидно е, че в наши дни социалните предприятия оказват силно положително влияние върху обществото като цяло. Нещо повече, те често се превръщат в буфер, който следва да предпази хората от възможните негативни последици, породени от различни икономически кризи.

> *"Социалното предприемачество е една от основните теми, които бяха обсъдени на Световния Икономически Форум, състоял се в Давос през януари 2017 година, разгледано като нов начин или инструмент за превъзмогване на определени социални проблеми, с които се сблъскват съвременните общества* [11]*."*

Важно е да отбележим, че бизнес средата постепенно се променя от по-традиционна офис среда в дигиталната такава, която позволява също така прилагането на различен бизнес подход от компаниите и която е далеч по-адаптивна към непрекъснатите промени в обществото. Дигиталната среда, иновациите и нововъзникващите технологии представляват възможности, които бизнесът трябва да вземе предвид при извършване на ежедневните си операции, но трябва да знаем, че последните могат да бъдат и потенциални заплахи, ако не бъдат приложени правилно. В случай, че искате тези инструменти да повлияят благоприятно на бизнеса ви, то те трябва да бъдат интегрирани в съответствие с посочените изисквания, като техният фокус следва да се насочи върху обезпечаването на мерки за управление на рисковете за дигиталната сигурност, както и върху изработването на стратегия за поверителност[1].

За съжаление, бизнесът често не разбира как дигиталната сигурност и въпросите относно сигурността могат да създадат икономически рискове, срещу които впоследствие е трудно да се реагира и те да бъдат управлявани. И докато различните видове малки и средни предприятия се сблъскват с различни предизвикателства, за всички тях би било от полза да въведат оценка на

рисковете за дигиталната сигурност и поверителността в техните процеси по вземане на управленски решения.

В настоящата дигитална ера услугите в различните бизнес отрасли трябва да се предоставят непрекъснато, 24 часа на ден и 365 дни в годината. И макар прогресът в ефективното предоставяне на услуги да е осезаем, благодарение на технологии като IoT, методите за извършване на кибератаки продължават своето усложнено и разнообразно развитие – дори що се касае до кибертероризъм. Това е причината, поради която системната сигурност се оказва от ключово значение при обезпечаване на развитието на бизнеса изобщо [2].

> *“Интернетът, социалните мрежи и уебсайтове, както и социалните медии са основните средства за постигане на успех и взаимодействие между социалните предприемачи. В годините след 2000г., Интернет се превърна в особено полезно средство за разпространяването на информация и достигането ѝ до широк кръг от поддръжници за кратки периоди от време, дори ако чисто географски тези са разпръснати. В допълнение следва да отбележим, че Интернет позволява обединяването на значителни проектни ресурси чрез използване на принципите на отворения код” [3].*

Както вече установихме, всички видове предприятия, а в това число и социалните предприятия трябва да се приспособят към скоростта на развитие, средата и изискванията на дигиталната ера, както и да адаптират техните продукти, услуги, партньорства и процеси към дигиталната среда. За съжаление, що се отнася до адаптирането им с дигиталния свят, предприятията често пренебрегват възможностите, които им се откриват при дигитализиране на своя бизнес. А може ли дигиталната среда да подпомогне вашия бизнес и с какво?

Примери в тази насока са използването на wiki модели или подходи за краудсорсинг – например чрез едно социално предприятие може да се обединят стотици хора от различни краища на една държава (или от множество държави), които да си сътрудничат по съвместни онлайн проекти (т.е. при разработване на бизнес план или маркетингова стратегия за работа в областта на социалното предприемачество). Ето списък на някои сайтове за колективно финансиране, които целят да дадат възможност на младите предприемачи да насърчават

постигането на социални цели. Тези сайтове за колективно финансиране събират средства за организации с нестопанска цел, както и за реализиране на техните проекти:

- 33needs е сайт за колективно финансиране на социални предприятия. Неговата цел е да се намерят такива организации, които са в състояние да предизвикат промяна и да им се осигури необходимото за постигането ѝ, включително нужните инвестиции за социалните предприемачи, социалните предприятия и изобщо за компаниите, които преследват постигането на социални цели. В тази платформа социалните предприемачи имат между 30 и 60 дни, за да постигнат своята цел.
- Buzzbnk е онлайн пазар, който свързва социални предприятия от всички сфери на живота с техни поддръжници и фенове. Buzzbnk изисква заплащането на ниска такса за регистрация, за да могат социалните предприятия да се присъединят към сайта.
- CauseVox е сайт за колективно финансиране, който се използва както от организации с нестопанска цел, така и от такива със стопанска цел. Този сайт най-общо ви предоставя определен набор от инструменти и шаблони, за да създадете своя кампания по набиране на средства, да приканите вашите поддръжници да ви подкрепят чрез вашия уебсайт или чрез социална мрежа, да следите прогреса си, както и да използвате правилно данните си.
- IndieGoGo предлага на всеки, който има идея — креативна, свързана с кауза или предприемаческа идея — инструментите за създаване на кампания и набиране на средства. Въпреки, че това е общ сайт за колективно финансиране, той се отличава с ясен фокус върху проектите с обществена полза.
- ioby ви помага да съберете нужните средства, както и нови доброволци за вашата кауза. Ioby насочва вниманието си към проблемите на околната среда в градските квартали, както и към всички значими проблеми на засегнатите общности.
- OpenIDEO е двигател за социално развитие и иницииране на социални промени. След публикуването на определено предизвикателство следват

трите му фази на развитие — вдъхновение, концептуализация и оценяване. Членовете на общността могат да допринесат за постигането на целта чрез много различни начини – от разработването на вдъхновяващи проучвания, снимки, скици и идеи, до създаването на бизнес модели и откъси от код.

- Start Some Good е сайт за социални предприемачи, предназначен за обединяването на определени общности и за събиране на средства, нужни за осъществяване на промяна. В този сайт кампании за набиране на средства могат да се публикуват както от организации със стопанска цел, така и от такива, които извършват дейност със нестопанска цел.

Уебсайтове като тези могат да помогнат на социалните предприемачи да разпространят своите идеи до по-широк кръг от хора, да помогнат със създаването и поддържането на такива мрежи от хора като тях, както и да се свържат с потенциални инвеститори, дарители или доброволци на организацията. Това помага на социалните предприемачи да постигнат своите цели, при това с много малък или без стартов капитал, а дори и без необходимите помещения (например нает офис място). Такъв пример представлява нарастващото влияние на технологията „отворен код“ като надежден инструмент, който позволява на хората по целия свят да работят съвместно за решаването определени регионални проблеми.

В последните години все повече се набляга на подкрепата за социалните предприятия в ранните фази на тяхното развитие – от началната концепция, през тяхното основаване и инвестиция. Често се използва терминът “инкубатори”, тъй като тези инициативи нерядко работят съвместно с лица или екипи, които имат идея за социално предприятие и осигуряват определени инструменти за подкрепа, за да помогнат за разработването и учредяването на предприятието. Някои от тези лица и екипи предоставят също така ежемесечна или ежегодна помощ за реализация на стартиращи проекти и организации [4].

СЪВЕТИ ЗА СОЦИАЛНИ ПРЕДПРИЕМАЧИ:

Възползвайте се от средствата, които предоставя съвместното работно пространство

Липсата на офис пространство често възпрепятства хората да започнат свой бизнес. Съвместните работни пространства решават този проблем, като ви дават място, където можете лесно и спокойно да работите съвместно. Наемите в съвместните работни пространства са по-ниски в сравнение с наемите на самостоятелни офиси. Друга възможност е да потърсите безплатни помещения или дори хъб за стартиращи компании, които могат да бъдат финансирани на местно, регионално или национално ниво и които предоставят безплатни офиси за стартиращи компании [5].

Използвайте безплатни услуги за осигуряване на приходи от вашия бизнес

Социалните предприемачи следва да популяризират своите предприятия чрез някои от многото безплатни услуги, появили се напоследък. Вече съществуват платформи, с които всеки един предприемач може да стане успешен, и то без да назначава продавач, дизайнер или цял екип, който да създаде неговия уебсайт. Тези уебсайтове представляват онлайн мобилни пазари, чиято цел е подбирането на труда на свободна практика в съответствие с местните нужди, позволявайки на потребителите и на предприятията да намерят необходимата подкрепа, когато такава им е нужда [5]. Ето някои сайтове, които помагат за осигуряване на приходи или за предлагане на определени умения онлайн: TaskRabbit, Crowdsite, Envato studio, …

Използвайте платформи за колективно финансиране

Социалните предприемачи могат да извлекат сериозни ползи от използването на платформи за колективно финансиране, като последните им позволяват да представят продукта си на глобалната сцена и да получат финансиране от всевъзможни места. Примери за такива платформи и уебсайтове вече бяха посочени по-горе [5].

Насърчавайте иновациите

Щом четете всичко това, то значи вие сте социален иноватор, но въпреки това е важно да не забравяте да насърчавате прилагането на иновации и да давате възможност на всеки един служител от вашата компания да има директен достъп до хората, които вземат управленските решения. Наемайте страхотни хора и им давайте възможност да бъдат иновативни. Иновативността не се състои непременно в следващата голяма идея; тя може да се заключава в начина, по който комуникирате или осъществявате бизнес процесите си, както и в технологията, която използвате. В този смисъл следва да разглеждате иновативността – като всичко или всеки, който подобрява вашите бизнес процеси, така че те да са по-добри, отколкото са били вчера. За да се превърнете в успешно дигитално социално предприятие, задължително условие е всички ваши бизнес процеси да бъдат оценени наново. Ако не направите това, то със сигурност няма да е налице синхрон по отношение на ефективността, достъпът до данни и предвидимостта на вашите процеси – обстоятелство, което ще доведе до забавяния и грешки, които са недопустими в настоящия дигитален свят [5].

> *“Дигиталните технологии разкриват едно ново и може би необятно поле за иновативни стратегии…” [11]*

Бъдете социален предприемач, който се води от данните

Вземането на решения, които са обосновани на основа на конкретни данни – това е ключът към успешното разрастване на бизнеса. Трябва да се възползвате от тези достъпни данни като използвате последните с цел да разберете кои неща работят по най-добрия начин. Малките промени от този тип могат да представляват огромен фактор за успеха на едно предприятие. Препоръчително е да използвате услуги като Google Analytics за засичане на статистиките на мрежовия трафик и Google AdWords, за да подобрите вашето SEO (оптимизиране на търсещите системи) с оглед избрания от вас пазар [5].

Направете поддръжниците на продукта ви част от екипа

Разберете кои са вашите поддръжници и използвайте последните, за да ангажирате определена общност с вашите продукти. След като веднъж вече намерите тези хора, някой от вас трябва да се постарае да ги държи ангажирани с вашите проекти. Ако едно лице харесва определен продукт, то той ще бъде и позитивно настроен към вашето предприятие, просто направете така, че този продукт да стане част от неговия живот и той да го сподели със своите приятели [5].

Влогърите и блогърите се превръщат в доста важни лица, тъй като те са в състояние да бъдат „посланици“ на определен продукт и да рекламират дадена компания, като по този начин сериозно разширяват кръга от потенциални последователи. Това не означава, че е задължително да имате такъв „посланик“, но последният би ви помогнал значително да ангажирате повече хора с вашия проект и да разширите обхвата на целенасочената аудитория.

C. Дигитална Имплементация (Цифрово изпълнение) на Концепцията за Социално Предприемачество

Социалното предприемачество е иновативна форма на предприемачество, която е с подчертаната цел за постигане на социална солидарност, сътрудничество и отговорно отношение към обществото и към хората като цяло [6]. Този вид предприемачество постепенно укрепна и се възприе като неделима част от света на бизнеса, което породи и необходимостта то да се адаптира към настоящия дигитален свят. Опасностите тук произтичат от факта, че различните предприятия и техните служители не могат да се приспособят толкова бързо към промените, които дигиталният свят и развитието на технологиите носят със себе си. Социалните предприятия не са по-различни в този аспект.

В настоящия непрекъснато променящ се пазар следва да се запитаме няколко въпроса: Как социалните предприятия оцеляват и се адаптират към дигиталната ера? В повечето социални предприятия хората погрешно смятат, че ако имат уебсайт или канали в социалните медии, това е напълно достатъчно. Истината е, че за да има едно предприятие цялостно присъствие на дигиталния пазар, нужно е то да се изправи срещу конкуренцията и, разбира се, да привлече максимално повече потребители към себе си.

> *"Поведението на потребителите в наши дни се развива с такива темпове, че много от предприятията не могат да поддържат това ниво на развитие. Традиционните фирми от всички сектори една след друга се провалят да предоставят на потребителите това, което последните желаят и очакват да получат в условията на дигиталната ера. Тези, които не могат да отговорят на изискванията, се сблъскват с нарастващото влияние на дигиталната ера. Макар и технологиите да променят начина, по който работят компаниите, съществуват някои важни стъпки, предприемането на които може да помогне на социалните компании значително."* [7]

Трябва да знаем, че няма такова нещо като универсален модел или програма за промяна и адаптиране на бизнеса към дигиталния свят, но въпреки това проучвания в областта извеждат някои ключови стъпки, които компаниите следва да вземат предвид в процеса на адаптацията им към дигиталния свят.

Обсъдете стратегията си: хората и организациите не могат да се променят, ако не са наясно и не разбират целта на изготвянето на комуникационна стратегия, която да подпомогне работата им в условията на цифрова икономика. Традиционната вътрешна офис комуникация не върши работа, ако вие и вашите колеги сте изцяло дигитализирани и си комуникирате по Skype, Viber, чрез имейли и дори чрез intranet. Заради това е важно стратегията за комуникация да бъде преоценена и адаптирана в съответствие с дигиталната среда, като под стратегия за комуникация разбираме всички такива стратегии, които едно социално предприятие може да има (с потребители, с акционери, със служители, както и с всички други заинтересовани лица) [8].

Изградете нови структури: Социално предприятие, което функционира в настоящия дигитален свят, може да се нуждае от по-различна организационна структура от тази на обикновено действащите предприятия. Тъй като фокусът в дигиталната среда се измества все повече върху неща като визуализация, фотография, видео, стрийминг и социални медии, то нуждата на предприятията от наемането на дизайнери, фотографи и видео редактори е доста по-голяма в сравнение с тази на обикновените социални предприятия. Поради това, тяхната организационната структура следва да бъде преоценена и допълнително проектирана така, че да отговаря на нуждите на организацията в условията на дигитална среда, което може да се изрази в създаването на нови структури или екипи, които да обезпечават различните дигитални операции и бизнес модели. [8].

Мислете екипно: Когато колективно се опитвате да измислите решение за определен проблем, препоръчително е да включите в този екип служители от различни отдели, които имат разнородни умения и задълбочени познания в сферата на организационната политика, комуникациите, анализирането и други. Имайте предвид, че едно подобно сътрудничество е далеч по-вероятно да бъде иновативно и успешно в търсенето на определено решение[8].

Експериментирайте и учете: Дигиталната иновация се изразява в използването и работата с данни по съвсем нови начини. В този смисъл дигиталните социални предприятия следва да функционират с нагласата за бързина на действията и експериментиране, а в резултат на това могат да развият по-бързата комуникация с потребителите и служителите си. [8].

Преосмисляне на информационните технологии: Много ИТ системи биват твърде бавни и недостатъчно гъвкави за дигиталния бизнес, а тъй като компаниите целят да обновят своята IT инфраструктура, тяхното желание е системите им да са гъвкави, скоростни и сигурни [8].

Съвети за Дигитална Имплементация:

- Power Text Solutions осигурява цял куп уеб-базирани самостоятелни инструменти за проучвания, като например категоризация на информацията и нейното обобщаване. Целта на тази платформа е да се превърне в система без прецедент, която подпомага съвместното сътрудничество по уеб проучвания.
- Google Wave – разработена, за да позволява на хората от целия свят да общуват, да си сътрудничат и да обменят почти всякакъв вид информация, и то в реално време.

D. Дигитални Заплахи и Възможности за Социалните Предприятия

Европейската комисия и Европейския икономически и социален комитет обръщат специално внимание на нуждата на социалните предприятия да използват възможностите на дигитализацията, чрез които да постигнат своите социални и екологични цели. *“Социалната икономика и социалните предприятия трябва да използват дигитализацията и дигиталните технологии като лост за икономическа и социална трансформация, както и за засилване на своето влияние в рамките на Европа” [9].*

Възможността, която дигиталните технологии предоставят, е далеч по-сериозна за малките и средните социални предприятия и бизнес общностите, чиито ресурси често не достигат. Надеждните дигитални инструменти в комбинация с прости, но интегрирани дигитални и ИТ стратегии, позволяват извършването на съществена оптимизация на ресурсите. *“Уверете се, че крайната цел на прилагането на ново решение е кристално ясна, че имате подкрепата на висшето ръководство, както и че всички ключови (значими) акционери са включени в изпробването на тези решения. Извършени правилно, те могат да ви спестят време и пари, както и да ви помогнат да се съсредоточите върху оказването на все по-голямо влияние” [10].*

Дигитални Възможности за Социалните Предприятия

+ потенциалната възможност да привлечете много повече аудитория в дигиталната среда.

+ социалните медии като средство за справка с данните на хората (интересите на лицата, техните нужди, мнения и настроения).

+ това е чудесен начин да накарате хората да говорят за вашата организация и нейната рентабилност.

+ безплатно разпространяване на съобщения до целевата аудитория.

+ възможност да имате онлайн магазин и да привличате клиенти от целия свят [7].

Дигитални Заплахи за Социалните Предприятия

- изисква доста време;

- допълнителни разходи за персонал, ако се управлява вътрешно;

- уязвимост към нарушения на сигурността (чувствителна лична и корпоративна информация);

- Измама/Фишинг, Малуер/Троянски коне, Софтуер за изнудване, Кибератаки;

- трудности при установяването на съответствие;

Полезен съвет в тази насока е, при адаптиране на предприятието към онлайн средата, да създадете вътрешен контролен списък на организацията си. Това не само ще направи прозрачни вашите политики, процедури и процеси, чрез които организацията се приспособява към дигиталната среда, но също така представлява и добър начин да видите слабите места в организацията си, тъй като ще бъде очевидно кои неща сте пропуснали или още са в процес на адаптация.

За предприятията в дигиталната среда е важно да имат подходящ и надежден хардуер, но най-важното е да използват сигурни софтуерни програми и да прилагат мрежови мерки за сигурност и политики като: антивирусни софтуери, пароли и криптиране. Много от хората, които работят на различни позиции в организацията, имат достъп до чувствителна информация или такава относно сигурността, които трябва да бъдат добре защитени не само от потенциални външни хакери, но и от извършване на евентуални злоупотреби от персонала на организациите. Простите и ефективни политики за използването на пароли и криптиране са препоръчителни като първа стъпка за защита на информация, данни и поддържане на определено ниво на сигурност. Организацията или по-специално директорът или законният ѝ представител трябва да запознаят всички служители с техните права в рамките на системата. В тези случаи трябва се обясни на отделните служители до кои файлове и данни последните имат или нямат достъп. Трябва също така да съществува механизъм, по който ако служител се нуждае от определена информация, която към момента не му се предоставя от потребител, тя да му бъде предоставена, като следва да е изяснено какъв е целият механизъм за получаване на такъв достъп и кое е лицето, което одобрява получаването му.

Високопоставени мениджъри, директори или някои важни служители могат да имат дистанционен достъп до компютърните сървъри и до съществуващите данни. В тази връзка, вашата организация следва да приложи политика, според която трябва да бъде изготвен списък с тези служители, който да включва също така документите и информацията, до които те имат дистанционен достъп. Всяка от горепосочените стъпки по отношение на дигиталната сигурност не би могла да бъде изпълнена и да функционира в случай, че организацията не е създала

свое звено за наблюдение на операциите. Ако организацията не определи ясна система за наблюдение, начело на която да е назначен определен служител и ако всички служители не са наясно с наказанията, които са предвидени за съответните нарушения, то в тези случаи изготвянето на контролен списък за заплахи е на практика безсмислен.

Е. Контролен Списък за Дигитална Сигурност

	✓
Мрежова Политика	
Антивирусна политика	
Политика за пароли	
Политика за кодиране	
Политика за дистанционен достъп	
Защита на данни	
Защита на лични данни	
Управление на потребителските правомощия	
Потребителско образование и информираност на служителите	
Управление на риска	
Наблюдение	

F. Терминологичен речник

Краудсорсинг – това е модел на финансиране, при който лица или организации получават определени стоки или услуги, включително идеи и финансиране, от голяма и бързо развиваща се група от Интернет потребители; При този вид финансиране отделните участници комбинират усилията си за постигането на един общ резултат. Следва да отбележим, че като модел за финансиране, краудсорсингът съществува още от преди навлизането в дигиталната ера (тоест "офлайн").

Дигитално предприемачество – Дигиталното предприемачество може да се определи като предприемачество, при което обаче някои или всички предприемачески дейности се извършват дигитално, но не посредством традиционните начини. Продукти, дистрибуция, работни места – всяка от тези и други дейности могат да приемат дигитална форма в предприемаческите начинания.

Дигитален (цифров) пазар – Интернет прави достъпни огромен брой продукти и услуги за хората по целия свят, като е нужно единствено да имате връзка с мрежата. За дигитални продукти като музика и софтуер разпространението вече става моментално, безплатно и глобално, като за разпространението им в световен мащаб е достатъчно само да бъдат представени в някой уебсайт.

Дигитално (цифрово) работно място – Обхватът на Интернет позволява на дигиталните предприемачи да се възползват от потенциални служители и партньори по целия свят и да работят с тях, без да се налага последните да се местят. Глобалните виртуални екипи могат да предложат някои значителни ползи за дигиталния предприемач, улеснявайки го при намирането и наемането на талантливи служители, насърчавайки културното многообразие и подобрявайки използването на ресурси, както и предлагайки повишена гъвкавост и отзивчивост в работата.

Софтуер с отворен код – това е компютърен софтуер, чиито програмен код може да се преглежда, променя и разпространява свободно. Софтуерът с отворен код като цяло се смята за по-безопасна алтернатива на софтуера със затворен код, тъй като разработчиците могат да тестват кода за „задни врати“.

Софтуерът за изнудване е вид злонамерен софтуер от крипто вирусологията, който заплашва да публикува данни на жертвата на атаката или пък ѝ блокира достъпа до тях, като иска от жертвата да плати откуп, за да си върне достъпа до данните.

Шпионски софтуер – това е софтуер, който събира информация за вашия компютър и затова как го използвате, а след това изпраща тази информация на някое друго лице по Интернет. Шпионският софтуер обикновено работи в сянка и често се инсталира сам на вашия компютър, често без дори да сте дали позволение или да знаете за тази инсталация.

Вирус – това е програма или код, който се възпроизвежда в другите файлове, с които е в контакт. Повечето вируси само се възпроизвеждат, въпреки че много от тях могат и да причинят вреда на компютърната система или на данните на заразения потребител.

G. Заключения и допълнителна информация

Социалните предприятия следва да се приспособяват към нуждите на постоянно променящата се дигитална (цифрова) икономика, за да се обезпечи нормалното им функциониране. Променящата се дигитална среда и напредването на технологиите се превръщат във важен аспект от дейността на предприятията, в който аспект трябва да бъдат разпредели значителна част от техните ресурси. Интересно е да се отбележи, че някои социални предприятия успяват да постигнат тази промяна с малки или изобщо без инвестиции и усилия, докато други се нуждаят от допълнителна помощ за този процес. Дигиталната среда принуждава различните социални предприятия да направят повторна оценка на своите бизнес стратегии и да ги променят, така че последните да са в съответствие с настоящата дигитална среда. Тя следва да включва оценка на всички бизнес процеси на предприятията, които са били създадени преди промяната в работната среда. Поради преосмислянето на стратегиите и определянето на нови такива, някои предприятия могат да се сблъскат и с промяна в организационните структури на своя персонал. Мобилността и гъвкавостта са качества, които са от особено значение, за да може служителите да са достатъчно добре подготвени в условията на дигитална икономика. За да се поддържа нивото на дигитална (цифрова) трансформация е нужно предприятията постепенно да въвеждат нови технологии, нови бизнес процеси, както и да обръщат особено внимание на поддържащите системи и сигурността. Въпреки това, истината е, че предприятията не могат да променят и адаптират пълноценно само своите хардуерни системи и процеси, без да заменят и част от своите служители. Ако работната среда се променя, то работната сила също трябва да се промени.

Ето някои допълнителни материали по темата:

Дигитална бизнес стратегия: поглед към следващото поколение прозрения **MIS Quarterly**	От социалното предприятие до социалната иновация **5th Italian Business Forum 2017**	Киберсигурност – заплахи, предизвикателства и възможности **ACS**

Дигитална сигурност: през призмата на финансовите услуги

Ernst & Young

Изграждане на дигитална, социална и иновативна екосистема в Европа

NESTA

Социални предприятия

EUROPEAN COMMISSION

Влиянието на дигиталния свят върху управлението и маркетинга

KOZMINSKI UNIVERSITY

Нови технологии и дигитализация: възможности и предизвикателства за социалните предприятия

EECS

Развитие на соц. предприятия : сравняване на добри практики

OECD

H. Библиография

[1] OECD, 2016 Ministerial meeting: Managing Digital Security and Privacy Risk for Economic and Social Prosperity, https://www.oecd.org/internet/ministerial/meeting/Managing-Digital-Security-and-Privacy-Risk-discussion-paper.pdf

[2] Growing a Digital Social Innovation Ecosystem for Europe (2015), European Union, https://www.nesta.org.uk/sites/default/files/dsireport.pdf

[3] Durieux, Mark and Stebbins, Robert (2010): Social Entrepreneurship for Dummies, Wiley Publishing, Inc., Hoboken, *http://socialnaekonomija.si/wp-content/uploads/2015/03/Social-Entrepreneurship-For-Dummies-Mark-Durieux.pdf*

[4] British council (2015): Social Enterprise in the UK – Developing a thriving social enterprise sector, https://www.britishcouncil.org/sites/default/files/social_enterprise_in_the_uk_final_web_spreads.pdf

[5] Rupa Rathee (2017): ENTREPRENEURSHIP IN THE DIGITAL ERA, Asia Pacific Journal of Research in Business Management, Vol. 8, Issue 6, June 2017 Impact Factor: 5.16, ISSN: (2229-4104), https://www.academia.edu/33640590/ENTREPRENEURSHIP_IN_THE_DIGITAL_ERA?auto=download

[6] Socialno podjetništvo za začetnike, Ljubljana: ŠOU

[7] Rossi, Ben (2016): How companies must adapt to the digital revolution, http://www.information-age.com/how-companies-must-adapt-digital-revolution-123461760/

[8] Harward Business Review, Is Your Company Adapting Fast Enough to Thrive in an Increasingly Digital World?, October 2017, https://hbr.org/sponsored/2017/10/is-your-company-adapting-fast-enough-to-thrive-in-an-increasingly-digital-world

[9] New technologies and digitalisation: opportunities and challenges for Social Economy and Social Enterprise, https://www.eesc.europa.eu/en/agenda/our-

events/events/new-technologies-and-digitalisation-opportunities-and-challenges-social-economy-and-social-enterprise

[10] Violo, Marc (2017): Digital Tool Box for Social Enterprises & Charities, https://medium.com/on-purpose-stories/digital-tool-box-for-social-enterprises-charities-b4bc3f4c4184

[11] Prodanov, Hristo (2018): Social Enterpreneurship And Digital Technologies, Economic Alternatives, 2018, Issue 1, pp. 123-138, https://www.unwe.bg/uploads/Alternatives/9_Prodanov_EAlternativi_en_1_2018.pdf

ЧАСТ III

ПРАВНИ ВЪПРОСИ ВЪВ ВРЪЗКА С ДИГИТАЛНАТА СИГУРНОСТ

Списък с абревиатурите

Абревиатура	Определение
ЕС	Европейски съюз
ОРЗД	Общ регламент за защита на личните данни 2016/679
ДПП	Директива относно правата на потребителите 2018/83
EPD	e-Privacy Directive (Директива относно електронната сигурност)
HTTP	Протокол за пренос на хипертекст
ДЧ	Държави-членки

A. Въведение

Създаването на добре функциониращ цифров единен пазар с устойчива европейска икономика, основана на данни, е един от основните приоритети на Европейския съюз. Това по същество означава, че следва да бъде създаден механизъм за ефективно и трансгранично свободно движение на данни. Европейските компании също значително насочват усилията и ресурсите си в областта на цифровите разработки (развитието на цифровите технологии) като започват да въвеждат цифрови бизнес модели, за да могат да се възползват пълноценно от данните и анализите на тези данни.

Безпроблемното функциониране на мрежовите и информационните системи по цялата територия на ЕС е от съществено значение за поддържане на работеща онлайн икономика и осигуряване на икономическо развитие. За тази цел ЕС работи над много различни проекти, които следва да насърчават кибернетичната устойчивост.

Все пак тези нови бизнес модели не могат „да виреят в дивата природа“. С цел да се извлекат максимални ползи от тях, трябва да се вземе предвид приложението на регулаторен режим. В настоящата глава ще се запознаете с европейската законодателна рамка в областта на цифровата сигурност. Първата част на главата е посветена на най-скорошните промени в законодателството на ЕС, които предизвикаха турбуленции в европейското общество – така наречения Общ регламент за защита на личните данни (ОРЗД). Обстойният анализ на Регламента е последван от преглед на Директивата относно правата на потребителите (ДПП), Директивата за електронната търговия (ДЕТ) и Директивата за електронната сигурност (ДЕС).

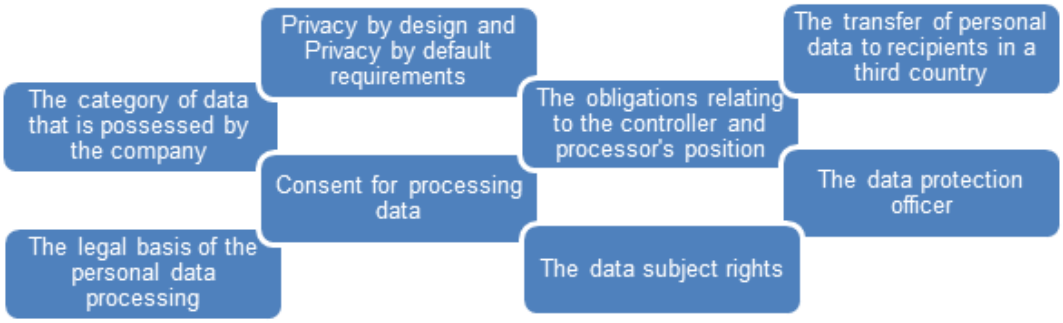
B. Насоки за защита на данните

В сила от 25 май 2018 година действат нови законодателни изисквания за всички компании, които обработват лична информация.

Може да се чували за Общия регламент за защита на личните данни 2016/679, познат също така като ОРЗД (GDPR). Това е регламент на ЕС, който е приложим по отношение на всяка компания, която прави бизнес с потребители в рамките на ЕС, предлага стоки или услуги на територията на ЕС, като има достъп до данни, имащи отношение към граждани на ЕС, включително и към техни работници. Основната цел на ОРЗД е да защити личните данни на гражданите на ЕС посредством стриктни изисквания, които оказват въздействие върху целия жизнен цикъл на данните и тяхното обработване в повечето организации. Тъй като се касае за огромен набор от правила и регулации, които уреждат използването на лични данни в рамките на ЕС, ОРЗД е от изключително значение за по-голямата част от бизнесите в региона.

Колко точно е важен ОРЗД за бизнеса може да се види по глобите, които са предвидени в случаите на неспазване на регламента. За несъобразяване с правилата на регламента, на всички организации, дори и тяхното седалище да е извън ЕС, могат да бъдат налагани глоби в размер до 20 милиона, или в размер на 4% от техния общ размер на приходите за предходната фискална година – в зависимост от това коя от санкциите е по-голяма. Това означава, че ако компания има потребители или служители в рамките на ЕС, изискванията на ОРЗД следва да бъдат приемани сериозно.

За да избегнете тези глоби, вие като предприемач или като част от компания трябва да сте в съответствие със следните изисквания на ОРЗД, които ще бъдат дискутирани в детайли по-надолу:



Фигура 1: Области, в които трябва да се постигне съответствие с ОРЗД

Лични данни

На първо място, за да се постигне съответствие с ОРЗД, от голямо значение е да се разбере коя информация или кои данни попадат под защитата на ОРЗД – или иначе казано, кои данни са лични данни.

Първо: не са лични данни тези данни, които се отнасят до юридически лица или починали физически лица.

Лични данни са всяка информация, която се отнася до субект на данни, който може да бъде:

- Физическо лице с *установена самоличност* – човек, който може да бъде разграничен от други членове на определена група, например чрез име или снимка;
- Физическо лице с *подлежаща на установяване самоличност* – човек, който може да бъде пряко или непряко идентифициран като например чрез използването на информация, която прави възможно установяването на неговата самоличност с разумни средства възможно – да речем чрез неговия/нейния глас или IP адрес.

Специални категории от лични данни, често наричани „чувствителни данни“, включващи лични данни, които разкриват:

Фигура 2: Специални категории лични данни

Поначало обработването на тези специални категории данни е забранено, освен ако субектът на данни не даде изричното си съгласие или ако обработването е по отношение на лични данни, които са публично изнесени от субекта на данни, както и в случаите, при които съществува законово задължение за обработването на този вид данни. В повечето случаи това задължение се отнася до обработването на данни във връзка със здравните досиета на хора.

Що се отнася до наемането на работа (трудовите отношения), съществуват някои изключения, тъй като работодатели имат правото (ако е нужно) да обработват „чувствителни данни“ на работниците и служителите си. Въпреки това, вие, като работодатели, следва да се уверите, че не съхранявате чувствителна информация, която позволява установяването на самоличността на работници за период по-дълъг от необходимия, като и не трябва да основавате, което и да е ваше решение изцяло на автоматизирано обработване и оценяване (включително профилиране).

Важна подкатегория на личните данни представляват псевдонимизирани данни, като това са данни, които не могат да бъдат свързани с конкретен субект на данни, без да се използва допълнителна информация, която допълнителна информация следва да е защитена и да се съхранява отделно. С други думи, това са лични данни, които са свързани с физическо лице с подлежаща на

установяване самоличност, чрез разумни средства (това, дали средствата са разумни, се определя от разходите и времето, които са нужни за установяване на самоличността, както и от достъпната технология през времето на обработване). Псевдонимизацията е начин за намаляване на рисковете, породени от и отнасящи се до обработката на лични данни.

От друга страна, анонимна информация е тази, чрез която по никакъв начин не може да бъде установена самоличността на субекта на данни – и нейното обработване не се регулира от ОРЗД. Следва да направим важно уточнение: данните могат да се считат за анонимни, само ако ре-идентификацията е на практика невъзможна, което означава, че ре-идентифицирането на определено лице следва да е невъзможно, от която и да е страна и чрез всички средства, които могат да бъдат използвани за такъв опит.

По-подробна практическа информация за това как се извършва псевдонимизация и анонимизация на данни се съдържа в Раздели IV и V от настоящото електронно ръководство.

Обработване

За да бъдете в съответствие с разпоредбите на ОРЗД, вие трябва да знаете какво представлява обработването на лични данни. Според Регламента обработване е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като **събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване**.

Това се прилага по отношение на всички напълно или частично автоматизирани системи, както и към напълно неавтоматизирани такива, които са част от регистър с лични данни или са създадени, за да бъдат част от такъв регистър. Определението на „регистър с лични данни“ е дадено в ОРЗД и означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е

централизиран, децентрализиран или разпределен съгласно функционален или географски принцип. Като пример за това какво представлява регистърът с лични данни можем да посочим дори визитните картички, които вашите бизнес партньори ви дават: събирайки ги във вашия визитник, вие създавате регистър с лични данни.

Следва още да бъде уточнено, че обработването на лични данни от физическо лице във връзка с **лични дейности или такива в рамките на домакинството,** които **не са във връзка с извършването на професионални или търговски дейности**, не попадат в приложното поле на ОРЗД. Например дори поддържането на кореспонденция във Фейсбук се счита за обработване на лични данни, но тъй като това обработване се извършва за лични цели, а не за търговски такива, последното не попада в обхвата на ОРЗД. Въпреки това, когато комуникирате с хора в социалните мрежи, но тази комуникация се извършва с търговска цел (например продавате определен продукт в Инстаграм), ОРЗД се прилага.

	ДА	**НЕ**
Отнасят ли се данните до физическо лице?	ОРЗД се прилага ✓	ОРЗД не се прилага ✗
Може ли чрез данните да се идентифицира физическо лице?	ОРЗД се прилага ✓	ОРЗД не се прилага ✗
Мога ли да отделя или изолирам идентифициращите данни от останалите?	ОРЗД не се прилага ✗	ОРЗД се прилага ✓

Планирам ли по някакъв начин да материализирам стойността на тези данни?	ОРЗД се прилага ✓	ОРЗД не се прилага ✗ (по отношение на лични дейности или дейности на домакинството)

Фигура 3: Резюме на приложението на ОРЗД

Основни принципи при обработването

Според ОРЗД всеки вид обработване на лични данни, който попада в приложното поле на Регламента, трябва да съответства на следните принципи:

Законност **Добросъвестност** **Прозрачност**	- **Обработване на данните според изискванията за законност, посочени в Чл.6 ОРЗД;** - **Информиране на субекта на данни за наличието и естеството на обработването;** - **Осигуряване на лесен достъп до информацията за обработването на лични данни, която следва да бъде написана на разбираем и достъпен език (вкл. информация относно самоличността на администратора и целите на обработването, както и рисковете, правилата, гаранциите и правата, свързани към обработването);** - **Информиране на субекта на данни за наличието на профилиране и неговите последици;** - **Информиране на субекта на данни, дали те са длъжни да предоставят лични данни и какви са последиците.**
Конкретни и подробни (изрични) цели **Легитимност**	- Ако лични данни се обработват за легитимни цели, посочете по конкретен и подробен начин кои са тези цели по време на събирането на данни; - Не продължавайте обработването на лични данни, когато то вече е несъвместимо със съответните цели;

	- Когато администраторът възнамерява да обработва лични данни за цели, различни от тези, с които последните са събирани, администраторът следва да информира субекта на данни (преди по-нататъшна обработка) затова какви са другите цели, както и за останалата нужна информация; - Това ново обработване следва отново да е съобразено с всички принципи.
Свеждане на данните до минимум **Ограничение на съхранението**	- Събраните лични данни трябва да бъдат подходящи, относими и ограничени само до това, което е нужно във връзка с целите на обработването; - Личните данни следва да се съхраняват във форма, която позволява идентификацията на субекта на данни за не по-дълго от необходимото време с оглед на целите, за които личните данни се обработват (изключение правят съхраняването на информация за постигане на цели в обществен интерес, за научни или исторически проучвания, както и за статистически цели, когато за съхраняването са взети специални мерки, гарантиращи правата и свободите на субектите на данни).
Точност	- Личните данни трябва да бъдат точни, а когато е нужно, следва да бъдат и актуализирани; - Използвайки разумни средства, постарайте се да коригирате или изтривате периодично всички неточни лични данни.
Цялостност **Поверителност**	- Осигурете подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане; - Осигурете гаранции, че обработваните лични данни са защитени от потенциални течове на информация, както и че личните данни нямат да бъдат загубени, повредени или унищожени;

	- В случай на инцидент, който нарушава горепосоченото, администраторът е отговорен за причинената вреда и от него може да бъде поискано обезщетение, ако не успее да докаже, че по никакъв начин не е отговорен за нанесената вреда и че всички подходящи технически и организационни мерки за защита на базата данни са били приложени; - За да осигурите подходящо ниво на защита, постарайте се да: o псевдонимизирате и криптирате личните данни; o гарантирайте съществуващите поверителност, цялост, наличност и устойчивост на обработващите системи и услуги; o обезпечете възможността за възстановяване на наличностите и своевременен достъп до данните в случай на инцидент; o редовно тествайте, анализирайте и оценявайте ефективността на техническите и организационните мерки за сигурност.
Уведомяване на надзорния орган	- Нарушение на сигурността на лични данни означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин. Нарушението може да е самостоятелно или комбинация от: o “Нарушение на конфиденциалността” – неразрешено или случайно разкриване или достъп до лични данни; o “Нарушение на наличността” – случайна или неразрешена загуба на достъп до или на унищожаване на лични данни; o “Нарушение на целостта” – неразрешена или случайна промяна на личните данни; - Уведомяването компетентния надзорен орган за нарушението (пробива) в сигурността на личните данни

	(орган по защита на данните) трябва да се направи в срок до 72 часа след узнаването за него; - Необходимо е на органа по защита на данните да се предостави информация за: естеството на нарушението; категориите и приблизителния брой на субектите на данни, както и съответните записи; име и данни за връзка с длъжностното лице по защита на данните; възможни последици от нарушението; предложени мерки. Ако има забавяне при уведомяването, последното трябва да се обоснове; - При нарушения, които не е вероятно да породят риск за субекта на данните, уведомяване на надзорния орган не се изисква (например при обществено достъпни лични данни или при хаширане и „засоляване“ на данни, които все още имат некомпрометиран ключ).
Уведомяване на субектите на данни	- Когато има голям шанс за пораждане на неблагоприятни ефекти вследствие на нарушението на данните, потърпевшите лица трябва да бъдат уведомени за нарушението веднага щом е разумно осъществимо; - Предоставяне на конкретна информация относно възможните последици и мерките, които трябва да вземат лицата, за да се предпазят, както и описание на естеството на нарушението, име и контакти за връзка с длъжностното лице по защита на личните данни или на друго звено за контакт; - Поддържа комуникацията ясна и открита, без да включва друга информация като например за регулярни ъпдейти, новинарски бюлетини и др.; - Използва повече от един канал за комуникация (СМС, имейл, уеб банери, видни реклами и др.), за да успее информацията успешно да достигне до засегнатите лица; - Не е нужно уведомяване на засегнатото лице, ако и трите долупосочени изисквания са налице кумулативно:

	○ Ако данните са неразбираеми за всеки човек, който няма разрешен достъп до тях (например, когато са криптирани сигурно); ○ Непосредствено след нарушението са предприети всички нужни действия, за да се гарантира, че вече не е вероятно рискът да се осъществи; ○ Свързването с всички лица поотделно би коствало непропорционални усилия (на първо място, контактите за връзка с тях са изгубени или неизвестни).
Риск и Висок риск	- След като нарушението се установи, важно е да се направи оценка до какъв риск може да доведе то, за да може да се разбере вероятността и тежестта на въздействие върху лицата, както и дали е нужно тяхното уведомяване; - Риск съществува, когато нарушението може да доведе до физически, материални или нематериални вреди за лицата, чиито данни са били обект на нарушението; - Критериите, които следва да се вземат предвид са: ○ Видът на нарушението; ○ Естеството, чувствителността и обема на личните данни; ○ Степента на сложност при установяване на самоличността на лицата; ○ Тежестта на последиците за лицата; ○ Особени характеристики на лицата; ○ Броят на засегнатите лица; ○ Особени характеристики на администратора.
Отчетност Водене на регистри	- Независимо дали има задължение за уведомяване, администраторът следва да пази цялата документация за всички нарушения на сигурността на личните данни; - Препоръчително е да се създаде вътрешен регистър с нарушенията, който да включва причините, описание на нарушението, последиците от него и предприетите действия за справяне с него;

	- Препоръчително е да се създаде и поддържа процедура, която да съдържа начините за ограничаване, справяне с и възстановяване от инцидентите, преценка на рисковете и необходимите уведомявания, като работниците и служителите следва да се информират за тази процедура.

Фигура 4: Основни принципи при обработването на данни

C. Насоки за защита на потребителите

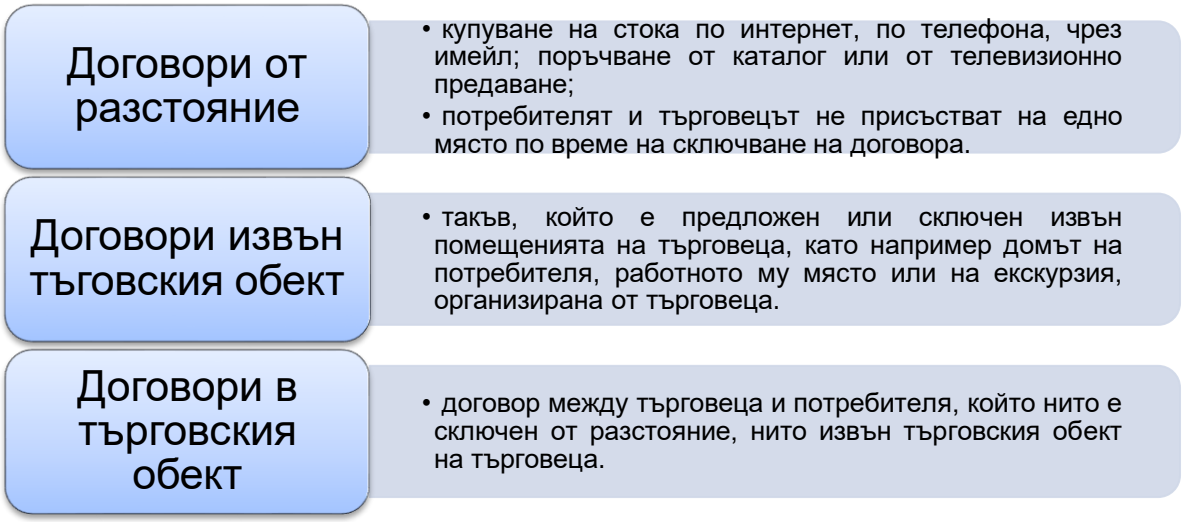
По подобие на начина, по който защитата на личните данни се регулира от ОРЗД, защитата на потребителите е уредена в Директива 2011/83/ЕС на Европейския парламент и на Съвета от 25 октомври 2011 година относно правата на потребителите (позната също като Директива за правата на потребителите). Тя отменя две предишни Директиви – първата (Директива 85/577/ЕИО на Съвета) за защита на потребителите във връзка с договорите, сключени извън търговски обект и втората (Директива 97/7/ЕО на Европейския парламент и на Съвета) относно защитата на потребителя по отношение на договорите от разстояние.

Целта на Директивата е да постигне високо ниво на правна защита на потребителите в рамките на ЕС и да допринесе за доброто функциониране на вътрешния пазар. Директивата се прилага по отношение на всички контакти, осъществени между търговец и потребител.

Държавите-членки (ДЧ) са задължени да я транспонират в тяхното национално законодателство до 13 декември 2013 г., а всички национални мерки за транспонирането ѝ следва да са приложени до 13 юни 2014 г.

Директивата се имплементира с максимална хармонизация, позната също като “пълна хармонизация”, което означава, че държавите членки не могат да въведат по-ограничителни мерки в тази област – правилата в Директивата са максимално приложимите. Директивата установява определени ключови права за потребителите и същевременно урежда правилата за сключване на договори между потребители и търговци, които оказват непосредствен осезаем ефект върху ежедневния живот на потребителите в рамките на ЕС.

Видовете договори, обособени от Директивата са три на брой: договори, сключени извън търговския обект; договори, сключени от разстояние; договори, сключени в търговския обект.



Фигура 5: Различни видове договори според Директива 2011/83/ЕС

По-нататък в Директивата договорите се категоризират на 4 различни вида: договори за продажба, договори за услуга, договори за предоставяне на цифрово съдържание и договори за предоставяне на обществени услуги. Класифицирането на един договор като договор за продажба или договор за услуга определя от кой момент започва да тече срокът за упражняване на правото на отказ от стоката (Член 9). Срокът за упражняване на право на отказ се определя като период от време, през който потребителят може да прекрати едностранно определен договор, без да посочва причини за това и без да заплаща никакви допълнителни разходи. За договори за услуги, за предоставяне на цифрово съдържание, както и за такива за предоставяне на обществени услуги, 14-дневният срок за право на отказ започва да тече от деня на сключване. Що се отнася до договорите за продажба, при тях срокът за отказ започва да тече от момента, в който потребителят влезе във владение на стоката (получи стоката).

Налице са специфични правила по отношение на продажбата на цифрови стоки като според Директивата всеки, който купува цифрово съдържание трябва да

получи ясна и недвусмислена информация за него, включително и детайли във връзка със софтуера и хардуера, с който съдържанието работи, както и информация за авторското право. В тези случаи потребителите следва да могат да се откажат от покупката на цифровото съдържание до момента, в който е започнало неговото изтегляне или излъчване.

Директивата изключва определени категории договори от приложението си, като например:

Фигура 6: Категории на дейностите, изключени от приложното поле на Директивата за правата на потребителите

Директивата за правата на потребителите накратко

Целта на Директивата е чрез нея да се постигне висока степен на правна закрила на потребителите в рамките на ЕС, както и да допринесе за доброто функциониране на вътрешния пазар чрез сближаване на определени аспекти от законодателствата на държавите-членки, регулации и административни разпоредби, отнасящи се до договори, сключени между потребители и търговци.

Какво значение има Директивата за бизнеса и потребителите се обобщава в таблицата по-долу:

Предимства за потребителите	– **Информацията, която следва да се предостави на потребителите преди да купят нещо и правото им да откажат онлайн покупка сега са еднакви за всички държави-членки на ЕС;** – **Потребителите могат да разчитат на едни и същи права, независимо в коя част на ЕС се намират;** – **Разширен кръг от права и по-голяма степен на правна закрила за потребителите, независимо от мястото и начина на извършване на покупка;** – **Пълна информация за крайната цена на продукт или услуга, включваща в себе си и допълнителни такси (разходи за доставка и др.).**
Нови правила за бизнеса	– Без повече „скрити разходи“ в Интернет: онлайн купувачите трябва да потвърдят, че са съгласни да платят за нещо преди да бъдат таксувани за него (цената трябва да е ясно определена). Потребителите не следва да плащат никакви такси, за които не са били изрично уведомени преди да извършат покупката; – Без повече предварително отбелязани онлайн полета: изрична забрана в Директивата е предвидена за предварително отбелязаните онлайн полета в уебсайтове, които таксуват с допълнителни плащания; – На търговците не е позволено да таксуват плащанията с кредитни карти по-скъпо, отколкото са техните разходи за предоставянето на подобна възможност;

	– Цените на разговорите с горещи линии за оплаквания и въпроси на потребители не трябва да бъдат по-високи от нормалните цени на такива разговори.
	Правила за обезщетяване: – Периодът, в който потребителите могат да се откажат от покупка, направена от разстояние (например онлайн) или от покупка, направена извън търговския обект (когато продавачът посещава дома на потребителя) се увеличава, като предишният минимум от 7 дни се променя на подсигурени 14 дни в рамките на ЕС; – Тези 14 дни започват да се броят от деня, в който потребителят получи стоката, като в този срок той може да се откаже от покупката, без да посочва причина. Когато продавачът не е информирал ясно потребителя за правото му да се отказва от направените покупки, срокът за връщане на покупката се удължава на една година; – Търговците следва да обезщетят потребителите в 14-дневен срок от направения отказ, включително и за разходите по доставка на стоката. По отношение на стоката, търговецът може да отложи връщането на покупната цена, докато стоката му бъде върната от потребителя или той представи, че последната е била изпратена на търговеца. Това правило не се прилага при ръчно изработени продукти, както и при нетрайни продукти (като например млечни продукти); – На потребителите се дава стандартен европейски формуляр, който да използват в случай, че решат да се откажат от покупките си,

	макар и да не са задължени да го използват. Ако търговецът иска потребителя да плати за връщането на стоката след направения отказ, той задължително трябва да го е информирал затова преди покупката и да му е представил приблизителната стойност на връщането.
Важни последици за бизнеса	– Общите правила за бизнеса правят търговията в цяла Европа по-лесна; – Търговците, които сключват продажби по телефона, по имейл, онлайн или извън техните помещения, трябва да спазват еднакъв набор от правила. Това създава равни условия за тях и намалява разходите по трансграничните сделки; – По отношение на малкия бизнес и занаятчиите, не съществува възможност за отказ от договор за извършаване на неотложни поправки или дейности по поддръжка. Държавите-членки могат също така да освободят търговците, които извършват ремонти или дейности по поддръжка в домовете на потребителите и за по-малко от 200 евро от определени изисквания за предоставяне на информация.

Фигура 7: Последици, произтичащи от Директивата за защита на потребителите

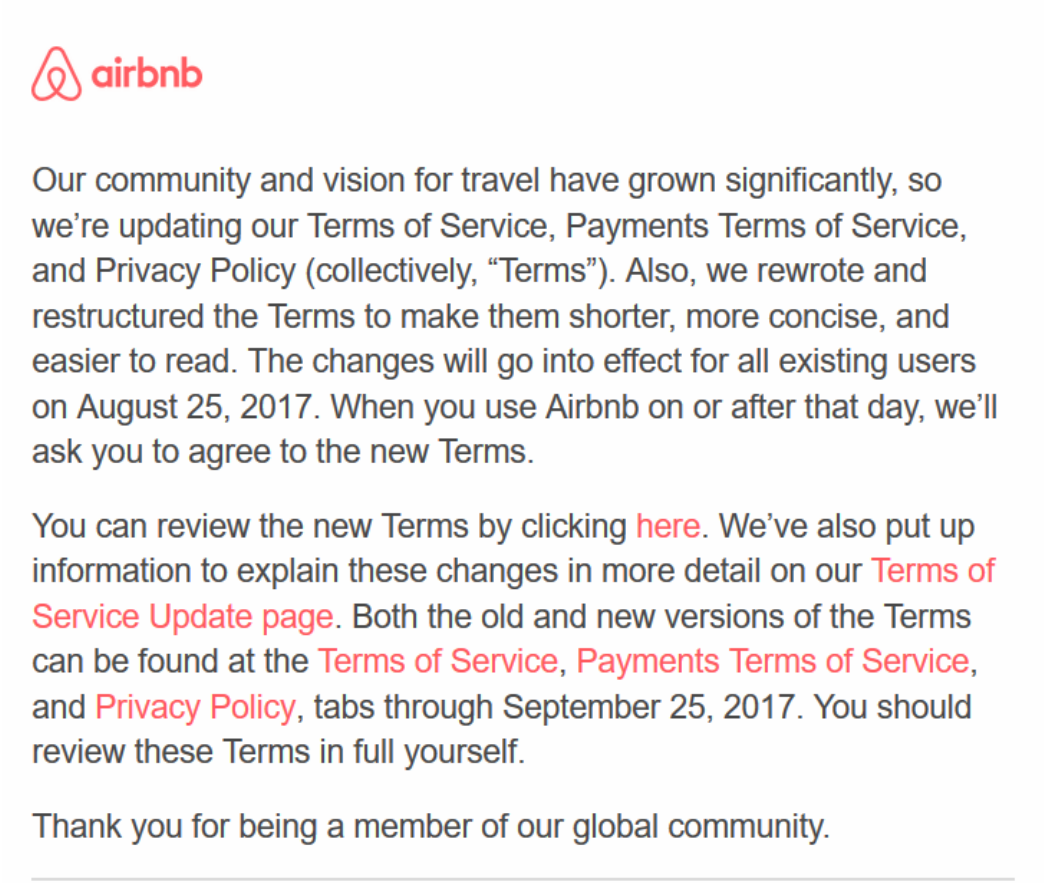
Съответствие на предприятията с Директивата

За да можете да бъдете в съответствие с всички аспекти на Директивата, ето няколко полезни съвета, които също така ще бъдат обобщени и включени в пълния списък със задачи в края на тази част от електронното ръководство.

1) Уверете се, че вашият уебсайт съдържа Общи Условия, които информират вашите потребители за всички техни релевантни права и задължения.

Част от тази информация следва да бъде включена и в Раздел „Правила за поръчка“ или на страниците, които потребителите използват за поръчване на стоки или услуги. Включете информация за сроковете за връщане, за възможностите за отказ, полагаемите обезщетения и др.

2) Когато бъдат направени някакви промени в Общите Условия, постарайте се да известявате клиентите си. Например след като Airbnb.com промени своите условия през юни 2017 година, клиентите получиха следния имейл:



airbnb

Our community and vision for travel have grown significantly, so we're updating our Terms of Service, Payments Terms of Service, and Privacy Policy (collectively, "Terms"). Also, we rewrote and restructured the Terms to make them shorter, more concise, and easier to read. The changes will go into effect for all existing users on August 25, 2017. When you use Airbnb on or after that day, we'll ask you to agree to the new Terms.

You can review the new Terms by clicking here. We've also put up information to explain these changes in more detail on our Terms of Service Update page. Both the old and new versions of the Terms can be found at the Terms of Service, Payments Terms of Service, and Privacy Policy, tabs through September 25, 2017. You should review these Terms in full yourself.

Thank you for being a member of our global community.

Съобщение за промяна на Общите условия:

В превод:

Нашата общност и визията ни за пътувания се разраснаха значително, поради което подновяваме нашите Условия за Ползване, Условия за Заплащане на Услуги, както и нашата Политика за Поверителност (накратко „Условия“). Също така, ние пренаписахме и променихме структурата на Условията си, за да ги направим по-кратки, по-стегнати и по-лесни за четене. Промените ще влязат в сила за всички настоящи

потребители на 25 август 2017 година. Това означава, че когато на следващия ден решите да използвате Airbnb, ние ще ви помолим да се съгласите с новите ни Условия.

Можете да разгледате новите ни условия като кликнете **тук.** Нещо повече, предоставили сме информация, за да обясним направените промени по-подробно, на нашата страница за Условия на Услугите за Актуализации. Както старата, така и новата версия на Условията могат да бъдат намерени на **Условия за Ползване, Условия за Заплащане на Услуги и на Политика за Поверителност.** Вие трябва да прегледате тези Условия изцяло и самостоятелно.

Благодарим Ви, че сте член на нашата глобална общност.

3) Създайте начин, чрез който потребителите да покажат, че разбират правата и задълженията си – това обикновено се прави с поле, което трябва да се отбележи преди регистрация или преди финализиране на поръчка.
4) Във връзка с предишната точка, запомнете, че предварително отбелязаните онлайн полета са напълно забранени.
5) Уверете се, че клиентите ви могат да се свържат с вас, без да дължат допълнителни такси (например с телефони с фиксирана тарифа и др.).
6) Осигурете лесно достъпен формуляр за анулиране на договора на вашите клиенти.

D. Насоки в електронната търговия

По начина по който защитата на личните данни се регулира от ОРЗД и защитата на потребителите се регулира от Директива 2011/83/ЕС, електронната търговия (е-търговия) се регулира от Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 година, известна също така Директивата за е-търговия.

Държавите-членки бяха задължени да я транспонират в националните си законодателства до 17 януари 2002 година. Целта на директивата е да създаде законодателна рамка за осигуряване на свободното движение на услугите на информационното общество между държавите-членки. Тя установява еднакви правила в рамките на ЕС по различни въпроси, свързани с електронната търговия. Тази Директива сближава определени разпоредби в националните законодателства на страните, отнасящи се до услугите на информационното общество и тяхното отношение с вътрешния пазар, установяването на доставчици на услуги, търговски съобщения, договори в електронна форма, отговорността на посредниците, етични кодекси, система за извънсъдебно разрешаване на конфликти, както и относно съдебни действия и сътрудничество между държавите-членки.

	Прилага ли се Директивата?
Новинарски услуги (като например новинарски сайтове)	✓
Продажби (книги, финансови услуги, транспортни услуги и др.)	✓
Областта на данъчното облагане	✗
Рекламиране	✓

Професионални услуги (адвокати, лекари, брокери на недвижими имоти)	✓
Хазартни дейности, които включват залагания с парична стойност в игри на късмета, включително лотарии и сделки, свързани със залагания.	✗
Дейностите на нотариусите или еквивалентни професии, доколкото съдържат пряко и специфично участие в упражняването на държавна власт	✗
Развлекателни услуги	✓
Въпроси, които се отнасят до услуги на информационното общество	✗
Основни посреднически услуги (достъп до интернет, предаване и приемане на информация)	✓
Безплатни услуги, финансирани от реклами, спонсорство и др.	✓
Въпроси, които се отнасят до споразумения или практики, уредени от антимонополното право	✗

Фигура 8: Приложение на Директивата за електронна търговия

Отговорност за посредниците

Директивата за електронната търговия съдържа няколко разпоредби относно отговорността на посредниците. Тя установява уеднаквени правила по въпроси като прозрачността и изискванията за предоставяне на информация от

доставчиците на онлайн услуги, търговски съобщения, договори в електронна форма и ограничения на отговорността на посредниците - доставчици на услуги.

“Обикновен Пренос”

Доставчици на услуги, чиято роля се състои само в пренасянето на информация, произхождаща от трети страни и в предоставянето на достъп до комуникационна мрежа, не отговарят за незаконно съдържание от трети страни, ако те:

- Не започват пренасянето на информацията;
- Не подбират получателя на пренесената информация; и
- Не подбират или променят информацията, която се съдържа в пренасянето.

Автоматичното, непосредствено и временно съхраняване на информация, ако това се прави при пренасянето на информация и с единствената цел за осъществяване на преноса на информация, също попада в обхвата на случаите, при които доставчиците се освобождават от отговорност.

“Кеширане”

Доставчиците на услуги не носят отговорност за незаконно съдържание от трети страни при предоставянето на условия за кеширане, при условие, че:

- Не променят информацията;
- Спазват условията за достъп до информацията и правилата за актуализиране на информацията;
- Не пречат на законното използване на технологията за получаване на данни за ползването на информацията;
- Действат експедитивно за отстраняване или блокиране на достъпа до съхранена информация, след като са узнали факта, че информацията е била отстранена от мрежата, достъпът до нея е блокиран или компетентните органи са наредили такова отстраняване или блокиране.

“Съхраняване на информация (Hosting)”

Доставчици на услуги, които съхраняват информация по молба на получателя на услугата и предоставена им от него, не носят отговорност, ако:

- Нямат сведения за незаконна дейност или информация, а във връзка с искове за щети, не е запознат с факти или обстоятелства, от които да е видна незаконната дейност или информация; или
- Доставчикът, при получаването на такива сведения или запознаването с такива факти, действа експедитивно за отстраняването или блокирането на достъпа до информацията.

Е. Бисквитки

Какво са Бисквитки?

HTTP бисквитката, също наричана уеб бисквитка, интернет бисквитка, браузър бисквитка, магическа бисквитка или просто бисквитка е малка част от данни, които се съхраняват на компютъра или мобилния телефон на потребителя и могат да бъдат разчетени с Notepad. Бисквитката дава възможност на уебсайта да "запомни" вашите действия или предпочитания в течение на времето (например, ако сте поставили продукти в онлайн кошницата си, ще имате достъп до тях при следващото си посещение на уебсайта). Бисквитката също така записва дейността на потребителите, включително история на кликовете, информация за влизане в профили, имена, адреси, пароли и други. Повечето браузъри поддържат бисквитки, но потребителите могат да решат дали да ги приемат, както и да ги изтрият по всяко време.

Различни видове бисквитки

Съществуват два основни вида бисквитки, разграничени по продължителността на живота им и по домейна, към който принадлежат. Те са:

- **Временни (сесийни) бисквитки** (in-memory cookie, временна бисквитка или нетрайна бисквитка) съществуват само във временната памет, докато потребителят използва сайта. Те обикновено се изтриват, когато потребителят излезе от браузъра.
- **Постоянни бисквитки** – стават невалидни на определена дата след определен период от време и в зависимост от домейна, към който принадлежат, за разлика от временните бисквитки. Информацията, която съдържат, се пренася на сървъра всеки път, когато потребителят посети уебсайта, към който принадлежат. Тези бисквитки са наричани също „проследяващи“ бисквитки, защото могат да бъдат използвани от рекламодатели за записване на информация относно навиците за търсене на техните потребители.

В зависимост от домейна, към който принадлежат, те се разделят на:

- **Първоразрядни Бисквитки** - тези, които са поставени от уеб сървъра на посетената страница и споделят един домейн, което означава, че домейнът на бисквитката ще съответства на домейна, който се показва в полето за адрес на уеб браузъра.
- **Треторазрядни Бисквитки** - тези, които се съхраняват на различен домейн от домейна на посетената страница. Този вид бисквитка обичайно е налице, когато уебстраници препращат към съдържание от външни уебсайтове, като например рекламни банери. Това създава възможност за следене на историята на търсене на потребителя и често се използва от рекламодателите, за да може да подберат подходящи реклами за всеки потребител.

Съществуват също защитени бисквитки, *бисквитки само за HTTP*, *супер бисквитки*, *зомби бисквитки*.

При нормални обстоятелства, бисквитките не могат да пренесат вируси или зловреден софтуер на вашия компютър. Това е така, защото данните в бисквитката не се променят, когато тя пътува напред-назад, затова и няма начин да повлияе на работата на компютъра ви. Въпреки това, някои вируси и зловредни софтуери могат да се маскират като бисквитки. Например “супер бисквитките” могат да бъдат потенциален проблем за сигурността, заради което и много браузъри ви предлагат да ги блокирате. “Зомби бисквитката”, от друга страна, е бисквитка, която се възстановява отново след като е изтрита, което прави справянето с нея трудна задача. „Проследяващи“ бисквитки от трета страна също могат да причинят проблеми със сигурността, тъй като последните улесняват и позволяват наблюдението на вашата онлайн дейност от трети страни, които не можете да идентифицирате.

Директивата за електронна сигурност

Използването на бисквитки предизвиква опасения за сигурността, поради което през май 2011 година беше приета Директива на ЕС за защита на сигурността на

потребителите онлайн. Това е Директива 2009/136/ЕО, която стана известна като Закона за Бисквитките (The Cookie Law) – Директива за е-сигурността. Тя е приложима за всеки човек или организация, със седалище в рамките на ЕС и имащи уебсайт и/или всеки уебсайт, който е насочен към потребители от ЕС и използва бисквитки.

Законодателството изисква сайтовете, които попадат в приложението му, да:

- ✓ Информират потребителите си затова, че използват бисквитки;
- ✓ Разясняват какви данни се събират с бисквитки и как се използват тези данни;
- ✓ Получат съгласието на потребителя за използване на бисквитки.

Ако притежавате уебсайт, вие ще трябва да се уверите, че той съответства на закона, което означава, че най-вероятно ще трябва да направите някои промени. Съответствието с Директивата за електронната сигурност се свежда до три основни стъпки:

- ✓ Информирайте потребителите си затова, че използвате бисквитки;
- ✓ Осигурете линк, на който могат да научат повече затова как използвате събраните данни;
- ✓ Осигурете начин, по който потребителите могат да дадат съгласието си за използването на бисквитки.

Най-често използваният начин затова е да се покаже малък банер в най-горната или най-долната част на вашия уебсайт, към който да има линк с подробна информация за сигурността/защитата на данните, както и бутон за даване на съгласие за използването на бисквитки и за скриването на банера.

Съществуват два вида съгласие, които уебсайтовете могат да изискват:

- **Изрично изборно съгласие** – потребителите трябва да кликнат бутон, да изберат отметка или да изпълнят някои други особени дейности, за да изберат кои бисквитки ще използват. Щом веднъж е дадено изрично съгласие, няма начин потребителите случайно да са се съгласили с използването на бисквитки

- **Мълчаливо съгласие** – най-честият начин за даване на такова мълчаливо съгласие като се покаже видимо съобщение относно бисквитките, което завършва със следното или подобно съобщение: "*С продължаване на използването на този сайт Вие се съгласявате с използването на бисквитки."* Важно е съобщението да е ясно изложено и потребителят да е наясно, че някои от специфичните действия ще бъдат възприемани като мълчаливо съгласие за използването на бисквитки.

Законодателството се прилага независимо дали потребителят използва компютър, смартфон, таблет или друго устройство. Поради това, когато настройвате съобщението относно бисквитките, важно е да се уверите, че съобщението се появява и функционира правилно на всички видове устройства.

ОРЗД и Бисквитките

Целта на ОРЗД е да защити "*физическите лица във връзка с обработването на лични данни и свободното движение на такива данни*". С други думи, целта е да се защитят потребителите на уебсайтовете. Бисквитките се споменават веднъж в съображение 30 от ОРЗД, като тези редове имат голямо значение за съответствието на бисквитките:

(30)

Физическите лица могат да бъдат свързани с онлайн идентификатори, предоставени от техните устройства, приложения, инструменти и протоколи, като адресите по интернет протокол (IP адреси) или идентификаторите, наричани „бисквитки", или други идентификатори, например етикети за радиочестотна идентификация. По този начин могат да бъдат оставени следи, които в съчетание по-специално с уникални идентификатори и с друга информация, получена от сървърите, може да се използват за създаването на профили на физическите лица и за тяхното идентифициране.

Иначе казано, когато чрез бисквитки може да се идентифицира едно лице, те се считат за лични данни.

Не всички бисквитки се използват по начин, по който потребителите могат да бъдат идентифицирани, но голямата част от тях попадат и ще попаднат в обхвата на ОРЗД. Това включва бисквитките за анализи, рекламиране и оперативни услуги, като проучвания и чат инструменти.

За да са в съответствие с изискванията, организациите ще трябва или да спрат да събират неотговарящите на закона бисквитки, или да намерят законно основание да събират и обработват тези данни. Повечето организации разчитат на съгласие (независимо мълчаливо или изрично), но завишените изисквания на ОРЗД означават, че ще е много по-трудно да се получават законни съгласия.

- **Мълчаливото съгласие вече не е достатъчно.** Съгласие трябва да се дава чрез ясно и недвусмислено потвърждаващо действие, като например кликване на прозореца с опции или избирането на настройки и предпочитания от менюто за настройки. Простото влизане в сайта не се счита за дадено съгласие.
- ***„С използването на този сайт, вие приемате използването на бисквитки“*** **– тези съобщения също не са достатъчни по същите причини.** Ако няма възможност за истински и свободен избор, тогава това не е действително съгласие. Трябва да дадете възможност както за приемането на бисквитките, така и за тяхното отхвърляне. Това означава, че:
  - **Оттеглянето на съгласие трябва да също толкова лесно, колкото и даването му.** В случай, че организациите искат да посъветват хората да блокират използването на бисквитки, ако последните не искат да дадат своето съгласие, на първо място те трябва да ги накарат да дадат съгласието си за използването им, тъй като само след това е възможно бисквитките да бъдат блокирани.
  - **Сайтовете трябва да осигурят възможност за оттегляне на съгласието.** Дори след като получат валидно съгласие, сайтовете трябва да предоставят възможност на хората да променят мнението си. Ако искате съгласието на потребителите чрез полета за избор в менюто с настройки, потребителите трябва винаги да могат да се върнат в това меню и да изберат отново своите предпочитания.

F. Контролен списък за законосъобразност

	✓
Моят уебсайт включва:	
Общи условия	
Права и Задължения	
БЕЗ предварително отбелязани полета	
БЕЗПЛАТНА форма за контакт	
Форма за отказ	
Не съхранявам „чувствителна“ информация за по-дълъг от необходимия период	
Знам какво представлява обработването на лични данни	
Когато обработвам лични данни, аз съм в съответствие с принципите на:	
Законосъобразност	
Прозрачност и добросъвестност	
Легитимност	
Свеждане на данните до минимум и ограничения при съхранението	
Точност	
Цялостност и поверителност	
Уведомяване на надзорния орган	

Съобщаване на субекта на данни	
Риск и Висок Риск	
Отчетност и Водене на регистри	
Предоставената от мен услуга / продукт предоставя пълна информация за разходите, включително всякакви допълнителни такси	
Не таксувам допълнително при плащане с кредитна карта	
Телефонът за клиенти е на цената на един градски разговор	
Потребителите ми са уведомени за използването на бисквитки	
Събирам съгласието на потребителите си за използваните бисквитки	
Обяснявам какви данни се събират при даването на съгласие за използването на бисквитки	

G. Речник на термините

Регламент на ЕС – Регламентът е законодателен акт на ЕС, който незабавно след приемането си влиза в законна сила като закон едновременно във всички държави-членки.

Директива на ЕС – Директивата е законодателен акт на ЕС, който изисква от държавите-членки да постигнат определени резултати, но без да определя средствата, които да се използват за постигането им. Тя се различава от регламентите, които са самостоятелно приложими и не изискват въвеждането на допълнителни мерки. Директивите обикновено дават на държавите-членки свобода на действие по отношение на това точно какви правила да бъдат приети. Директивите могат да бъдат приложени чрез различни законодателни способи в зависимост от предмета на регулиране.

Мерки по транспониране – В правото на ЕС, транспонирането е процес, при който държавите-членки на ЕС въвеждат разпоредбите на директива чрез прилагането на подходящи мерки по изпълнение. Транспонирането обикновено се извършва от първичната или вторичната законодателна власт.

Вътрешен пазар – Познат също като Европейски Единен Пазар или Пазар на Общността, Вътрешният пазар е единен пазар, който се стреми да гарантира свободното движение на стоки, капитали, услуги и работна ръка – „четирите свободи“ – в рамките на ЕС.

Съответствие – съответствие с действащото законодателство, независимо дали то е национално или международно.

H. Изводи и допълнителна информация

В тази глава от електронното ръководство се изложи в детайли нужната информация относно Общия Регламент за Защита на Данните (ОРЗД, последвана от анализ на Директивата за Правата на Потребителите (ДПП), Директивата за електронната търговия и Директивата за електронната Сигурност (ДЕС).

Въз основа на обсъжданите въпроси и след изпълнение на контролния списък, вашият бизнес вече е в съответствие със законодателните регулации в ЕС. Важно е никога да не се пренебрегват разпоредбите в националното законодателство и тези в правото на ЕС, тъй като това не просто ще ни направи спокойни, че няма да бъдем глобени, но и ще спомогне да станем социално отговорни търговци.

Адвокатските консултации често се приемат за скъпи и трудни за възприемане, но въпреки това се постарайте да се консултирате с хора, които са наясно какво е нужно на бизнеса, за да е в съответствие с настоящите изисквания и да избегнат простото приемане на някакви неясни правила, само за да избегнат плащането на по-големи разходи – тези ‘вратички’ могат да ви костват много повече за в бъдеще!

За още безплатни наставления и съвети по темата, може да използвате менторската платформа DiFens, достъпна на http://www.difens.eu/, където експерти по правни въпроси също могат да ви помогнат за вашия конкретен случай.

Още допълнителна информация:

Готови ли сте да отговорите на утрешните изисквания за защита на личните данни?

FORBES

Законен ли е вашият уебсайт?

YFS Magazine

Жизненият цикъл на защитата на лични данни се развива. Ето какво трябва да знаете.

FORBES

Законови изисквания за електронната търговия

EUROPEAN COMMISSION

Резюме на законодателните промени в сферата на електронната търговия по света

UNCTAD

Защо използването на бисквитки е от жизнено значение за бъдещето на мобилните технологии?

CLEARCODE

I. Източници

Competition and Consumer Protection Commission (2017) The Consumer Rights Directive: A guide for traders dealing with consumers. Available from: https://www.ccpc.ie/business/wp-content/uploads/sites/3/2017/03/CRD-Guidance_FINAL.pdf

European Commission (2014) DG JUSTICE: Guidance document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. Available from: https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf

Jelowicki, L. (2014) The EU Consumer Rights Directive 2014 explained. Practicology.com. Available from: https://www.practicology.com/thinking/blog/eu-consumer-rights-directive-2014-explained

Lindahl, F. (2013) The Consumer Rights Directive. Improved as a cross-border-only Regulation and toward a European Consumer Code, influenced by the Common Frame of Reference? Master's thesis in Commercial and Tax Law. Jönköping International Business School. Available from: https://www.diva-portal.org/smash/get/diva2:623054/FULLTEXT01.pdf

Schmon, C. (2016) Review of the Consumer Rights Directive. BEUC Comments. Available from: http://www.beuc.eu/publications/beuc-x-2016-093_csc_beucs_comment_to_review_of_consumer_rights_directive.pdf

Част IV

КИБЕРСИГУРНОСТ

J. Въведение

Съществуват много определения за Киберсигурност, като най-известното от тях е: “**Компютърна сигурност**, позната също като кибернетична сигурност или **ИТ (информационна) сигурност**, представлява защитата на **компютърни** системи от кражба или повреждане на техния хардуер, софтуер или информация, както и от нарушаване или погрешно насочване на услугите, които се предоставят от тях”[1].

Киберсигурността е една необятна и същевременно интересна област за провеждане научни изследвания в сферата на Компютърните науки (Информатиката). В настоящата глава ще обърнем най-голямо внимание на практическите аспекти на Компютърната Сигурност, или иначе казано как Компютърната Сигурност намира приложение в ежедневието ни. По-специално ще се занимаваме със сигурността на непрекъснатите бизнес процеси, включително най-малките и най-новите от тях.

Обикновено съществуват свойства, които влияят на работата на компютърните системи, като те могат да бъдат свързани с хардуера, софтуера или дори с мрежата. Понижаването на функционалността на това свойство може да доведе до последици като кражба, повреждане, нарушаване или погрешно насочване на информацията и процесите, свързани с бизнеса. Ослабеното действие на това свойство може да бъде умишлено – да се касае за съзнателна атака, или инцидентно – да става въпрос за повреда (техническа грешка). В най-честия случай това е вследствие на преднамерена атака, чиято цел е да се отслаби защитата на определена компютърна система.

Звучи като плашещ и сложен проблем, и общият случай наистина е такъв. Въпреки това хората не бива да се паникьосват или да действат прибързано. Използването на всички съществуващи проверки за сигурност, едновременно може да бъде също толкова безполезно, колкото и това да бездействаме. Наличието на твърде много мерки за сигурност повдига някои въпроси относно възникването на възможни проблеми. Първо, това означава, че ще натоварите с допълнителна работа вашите отдели, отговарящи за сигурността и по-специално за информационната сигурност. Тъй като сте предприемач, може би нямате

служители, които да се занимават само и изключително с това, което пък в случая може да доведе до изразходването на твърде много време и пари с цел наемането на външен партньор, който да ви осигурява нужните мерки за сигурност и софтуер. На второ място, ще трябва стриктно да изпълнявате твърде много мерки за сигурност, като това ще натовари допълнително служителите ви. Ако например всеки път те трябва да изпълнят многобройни стъпки, за да се свържат със софтуера за издаване на фактури, това ще затрудни допълнително тяхната работа и ще направи процедурите по-продължителни. Винаги съществува възможността хората да се опитат да намерят по-лесно решение на проблема или иначе казано „да му намерят цаката“. Тези решения обаче най-вероятно ще са тотално несигурни и неподходящи за прилагане. От друга страна, за бизнеса е много важно да се намери подходящият баланс между сигурност и производителност, като важен аспект, който влияе на производителността е така наречената „използваемост“. Конфигурирането на сигурността в софтуера и изработването на решения, които я гарантират, се оказва трудна задача за много потребители. Начинът, по който аспектите на сигурността са представени, особено що се отнася до техния дизайн и използваемост, правят конфигурирането да изглежда като сложен процес, който потребителите предпочитат да избегнат, а за съжаление в повечето случаи дори да игнорират [21]. Съществуват доклади, които посочват човешката немарливост като една от най-честите причини за възникването на грешки в конфигурацията за сигурност; като те се дължат предимно на неизползваемия дизайн на системите за сигурност [21] [22]. Нещо повече, използването на системи за сигурност, при които липсва тази използваемост, може да доведе до грешки на потребителите, които да компрометират цялостната сигурност [23].

Всичко от гореизброеното може да бъде преведено към разходите за дадена фирма. Очевидно е, че съществува нужда от създаване на по-гъвкави решения, които да осигурят персонализирани методи за обезпечавани на сигурността в зависимост от специфичните нужди на всяка фирма или организация. В тази връзка можем спокойно да кажем, че съществуват различни аспекти, които трябва да се вземат предвид при прилагането на системи за компютърна сигурност.

Друго нещо, което си заслужава да се спомене е това, че сигурността в една фирма, която се занимава с цифрови данни и тяхното обработване, следва да обхваща не само техническите аспекти, но и физическата част. Нека не забравяме, че компютърните системи се състоят и от хардуерни устройства, които могат да бъдат откраднати или унищожени по някакъв начин. Определени мерки за сигурност могат да бъдат взети с цел предпазването им - например съхраняването им в подходящи помещения, винаги да се заключва стаята, в която се намират и други. Физическата и техническата (виртуалната) сигурност в общия случай могат да бъдат съчетани, за да се предоставят адекватни решения при възникване на определени проблеми. Така например, ако лаптоп е откраднат или сървър е унищожен поради пожар, в случай, че правилно сте архивирали данните си, вие ще можете да ги възстановите и да подновите работата на системата си чрез друго хардуерно устройство. В този случай може и да има някаква загуба на данни, но тя няма да е фатална за бизнеса ви.

Една допълнителна стъпка, която всяка фирма може да предприеме, е да отдели време за обучение на потребителите си (в това число на служителите, доставчиците, както и всички останали, използващи системата) относно това защо и как трябва правилно да използват мерките и средствата за сигурност. Тази мярка може да им спести време за работа от този момент нататък, да откаже потребителите от опитите им да намерят решение на проблема, както и да ги информира по отношение на сигурността в работната среда.

Киберсигурността действително е много важна, но не само поради възможните загуби на данни, време или пари, които една фирма може да понесе в случай, че се сблъска с пробив в сигурността, но и заради Регламентите на ЕС, които уреждат защитата на личните данни и с които фирмите ще трябва да се приведат в съответствие, когато ОРЗД влезе в сила на 25 май 2018[19]. Несъответстващите на Регламента фирми могат не само да претърпят финансови загуби, но също и да са принудени да потърсят правна помощ, да им бъдат наложени глоби и да бъдат заведени дела срещу тях.

В следващите секции ще ви представим следните теми: Дигиталната сигурност като технически проблем, Влияние на пробивите в цифровата сигурност върху

процесите в бизнес средата, Решения относно Киберсигурността и заключение с Контролен списък по Киберсигурност и Терминологичен речник.

K. Дигиталната Сигурност като Технически Проблем

I. Въведение

Като за начало следва да отбележим, че Киберсигурността е не само технически проблем. Какво ще стане например, ако цялата телекомуникационна система се срине? Такъв срив би засегнал не само техническата част на бизнеса, но също така и процеси като извършването на продажби или покупки, инвентаризация, комуникация с клиентите и други.

Както вече се посочи по-горе, техническите аспекти на Киберсигурността могат да окажат непосредствено влияние върху целия бизнес. Това е практическата страна на Киберсигурността, поради което придобиването на повече знания относно техническите ѝ аспекти, е фундаментално за справянето с подобни кризи.

Различните приложения имат различни изисквания за сигурност които могат да бъдат групирани в следните принципи: Конфиденциалност, Цялостност, Годност, Заверяване, Отчетност, Поверителност и други. Трите най-важни принципа, наричани още триадата на ЦРУ, са Конфиденциалност, Цялостност и Годност на информацията. Компютърните системи, използвани в бизнеса, трябва да бъдат защитени на всички три нива по всяко време, като неспазването на някой от тях поражда по-голям риск за сигурността на вашата система.

II. Триадата от принципи на ЦРУ

Както вече обяснихме по-горе, от особена важност е всеки път, когато се опитваме да анализираме, оценим или приложим мерки за сигурност, в която и да е компютърна система, да се вземат под внимание всички принципи от триадата на ЦРУ. По-долу всеки от тях е описан по-подробно, за да може да се осигури по-доброто разбиране на материята.

Конфиденциалност

Принципът за Конфиденциалност се изразява в това, че информацията не е достъпна и не се разкрива пред неоторизирани лица, системи или процеси. Казано с прости думи, нещата, които следва да бъдат пазени като тайна, наистина трябва да бъдат тайна. Как можем да ги защитим? Колко е важно да ги защитим? Могат ли тези тайни да бъдат използвани срещу свързано лице? За да илюстрираме горепосоченото, представете си, че някой краде информацията за кредитните карти на клиентите на вашия онлайн магазин. Нещо повече, съществуват много други видове данни, които по принцип следва да се държат в тайна – интелектуална собственост, финансова информация, държавни тайни, лични данни на учениците/студентите и други. Принципът за конфиденциалност е от особено голямо значение, като редица закони и други нормативни актове са базирани на него. Щетите, които има възможност да бъдат нанесени поради липса на конфиденциалност, например вследствие на пробив в защитата на личните данни, могат да бъдат изключително сериозни. Това е най-ценният принцип от триадата на ЦРУ и този, с който хората обикновено са най-запознати. Съществуват ежедневни примери затова как прилагаме и осигуряваме Конфиденциалността. Един такъв пример е използването на криптирани канали за комуникация по интернет, както в ситуацията, при която трябва идентификационните данни за вход да преминат през “https” вместо през “http”, за да се запази комуникацията между клиента и сървъра напълно криптирана, а степента на конфиденциалност да остане висока. Собственикът на уебсайт трябва да се сдобие със сертификат за “https” и да го приложи с цел да постигане на сигурна комуникация. Криптирането вече се прилага при https протокола. Както се посочва в скорошно изявление на Гугъл: От юли 2018 г. насам, с пускането на Chrome 68, Chrome ще маркира всички “http” сайтове като несигурни (ненадеждни)”. Прочетете повече в официалното съобщение на Гугъл [8].

Като друг пример може да се даде използването на Виртуална Частна Мрежа - VPN мрежа, към която да се свържем, ако пътуваме, вместо просто да използваме някакви налични, но несигурни wi-fi мрежи. VPN е „тунелна мрежа, защитена чрез мрежа с голям обхват (WAN), като например Интернет, която предоставя сигурна комуникация между крайните си точки. Човекът, който е

свързан VPN, е в действителност сигурно свързан към защитена локална мрежа (LAN) на своята отдалечена фирма, което означава, че той/тя не е задължително да са разположени в близост до физическото разположение на локалната мрежа на фирмата, за да бъде мрежата сигурна [2]. VPN осигурява възможност за криптиране на комуникацията между клиент и сървър като мрежата е собственост на организация, която отговаря за кода и следенето на трафика, който минава през нея. В случай на атака, организацията ще може да намери чрез VPN мрежата исканията, които са подадени от и към нея, като в общия случай това ще разкрие кой е атакуващият.

Друг пример за осигуряване спазването на принципа за Конфиденциалност е използването на криптиращ софтуер с цел да се защитят определени обеми от данни. Такъв софтуер е „BitLocker“, който е технология, разработена от Windows, както и „FileVault“, който е съответното разрешение на MAC. Криптирането всъщност може да се разбира като технологична имплементация на принципа за Конфиденциалност. Наличието на данни с голямо значение, които са криптирани, може да помогне последните да останат тайна, дори и да бъдат откраднати, тъй като файловете ще бъдат нечетливи за всеки, който не притежава подходящия ключ за декриптирането им.

Съществуват няколко вида алгоритми за криптиране и методи, които могат да бъдат използвани за криптиране и защита на вашите данни. AES е най-известният и най-новият такъв метод. Но как могат да бъдат използвани тези възможности?

Както е илюстрирано във Фигура 1 по-долу, стъпките са както следва:

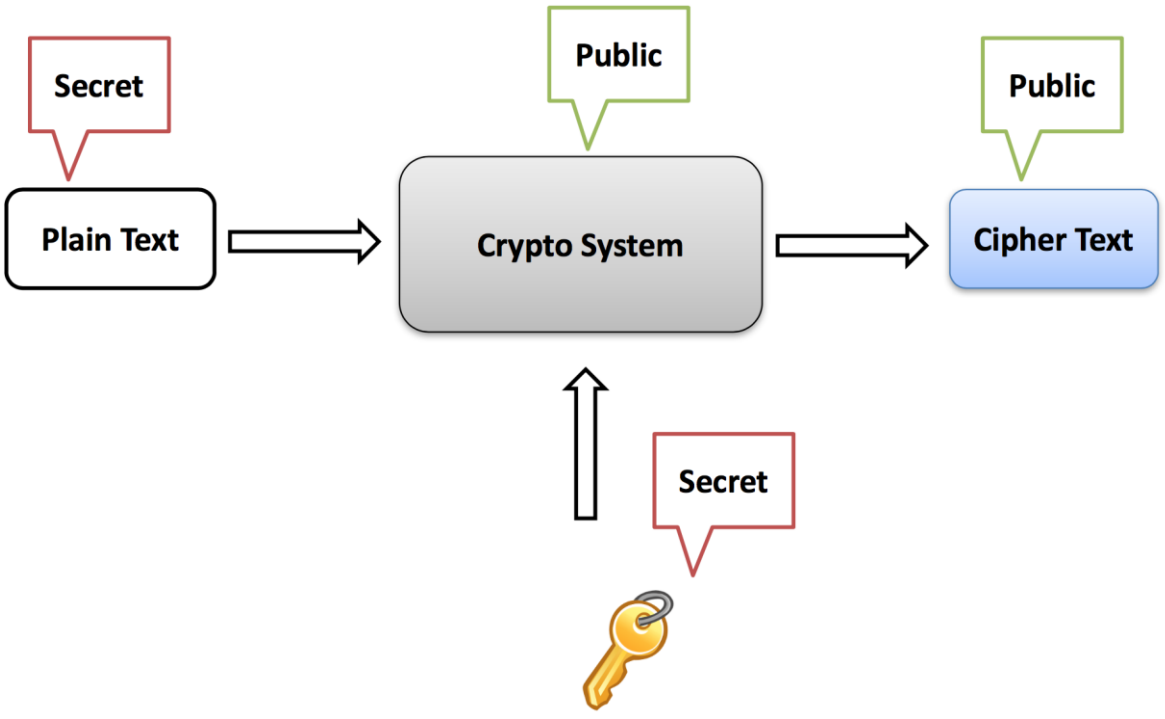
Първо, трябва да изберете криптографски алгоритъм (алгоритъм за криптиране), който да се приложи, като той трябва да включва Крипто системата. Криптографският алгоритъм е общодостъпен и е познат на всички, без това обаче да засяга сигурността на криптирането.

Второ, изберете ключ за криптиране, който ще направи данните нечетливи. Ключът вече определено трябва да се държи в тайна за разлика от криптографския алгоритъм.

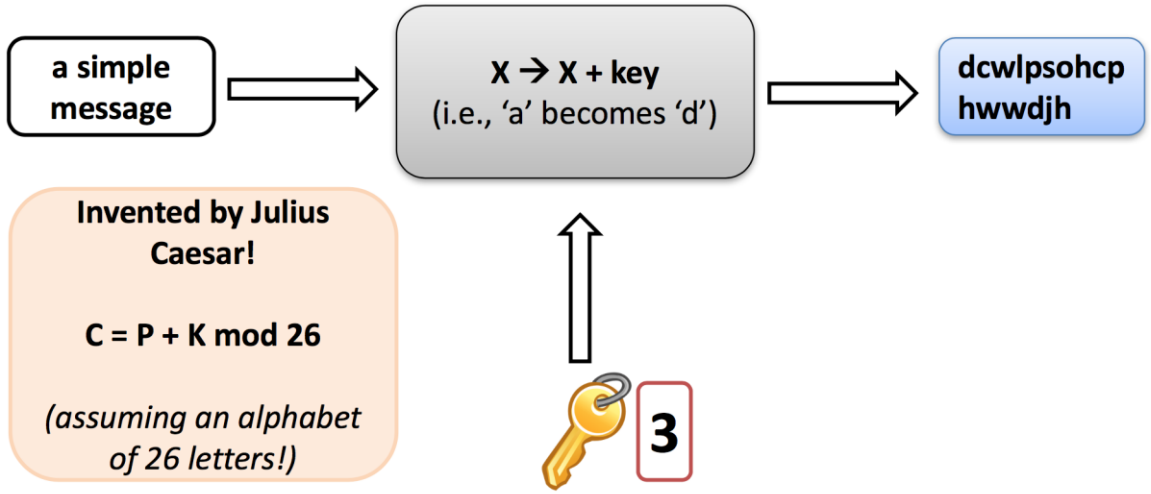
Като следваща стъпка, имайки ключа и информацията, която искате да криптирате, вече може да въведете последните в Крипто системата, която ще преведе данните в криптирани такива, наречени криптиран или шифрован текст.

Вече можете да изпратите или да съхранявате този криптиран текст. Дори и той да е общодостъпен, никой няма да може да го разчете, ако няма ключа за декриптиране.

Ако искате да използвате криптираните данни, то трябва първо да ги декриптирате като използвате съвместимия ключ.



Фигура 1 ([6])



Фигура 2 ([6])

Нека предположим, че имаме следния текст, който искаме да криптираме: “a simple text”. Към момента текстът е разбираем и за всички е ясно какво казва. Ако някой получи неоторизиран достъп до сървъра, за да прегледа или придобие данни от него, той/тя ще види текста „a simple text“. Сега избираме да използваме Caesar Cipher като наш криптографски алгоритъм. Този алгоритъм най-общо казано се състои в заместване на всяка буква само с една и съща друга буква в целия текст. След това решаваме, че нашият ключ ще е числото „3“. Моля, имайте предвид, че докато ключовете трябва да бъдат сложни, този е прост с цел да бъде използван за пример. За да бъдат в определен цикъл, всеки знак в текста „a simple text“ ще бъде преместен с +3 букви. В началото разделяме ключът (k=3) на 26 (буквите в английската азбука). След това преместваме буквата според остатъка при делението и така нататък. Като резултат от това, ние ще получим съобщението: “dcwlpsohcp hwwdjh”. Това съобщение вече определено не е четимо! Можем да го съхраняваме спокойно или да го изпратим някъде. Ако искаме да прочетем това съобщение като използваме нашия ключ, то трябва просто да приложим гореописания процес на обратно. Това означава, че следва да извадим нашия ключ от всеки от символите и т.н. [Фигура 2]

Нека сега видим как измерваме нивото на сигурност на криптиращия ключ с помощта на пример. Brute-force атаките в общи линии означават опитване на всички възможни комбинации, за да постигнем нещо определено (например за разбиване на парола или намиране на криптиращ ключ с диапазон от възможни комбинации). Криптиращият ключ, който е дълъг 4 бита, има 2^4 възможни комбинации, което се равнява на 16 опита, за да се разбие криптирането. Това е доста лесно в сравнение с 32-битовият криптиращ ключ, който има 2^{32} възможни комбинации, за разбиването на чието криптиране са нужни 4 294 967 296 опита. Ако ви звучи трудно, сега си представете какво ще е ако използвате дори по-голям, 64-битов ключ! Разбиването на такъв ключ ще отнеме толкова много време, че на практика се счита за невъзможно да се направи. Сега разгледайте отново нашия пример във Фигура 2, където използваният ключ се нуждае само от 2 бита, за да се представи: с 2 бита ние можем да имаме число от 1 до 3 или само $2^2=4$ комбинации. В такъв случай атакуващ, който използва brute-force атака, ще се нуждае в най-лошия случай от само 4 опита, за да намери нашия ключ.

Смятаме, че до този момент би трябва вече да е напълно ясно защо следва да сме в съответствие с принципа за Конфиденциалност. Той може да ни защити от хора, които умишлено или по невнимание получават достъп до наши секретни или чувствителни данни, като по този начин осигури достъп до тези данни само на оторизирани лица.

Цялостност

Принципът за цялостност определя, че данните или информацията не са променяни, унищожени или повредени, както и изгубени или променени по някакъв начин, независимо дали става дума за случайни действия или преднамерени неоторизирани такива.

Казано с прости думи, информацията следва да се поддържа в прецизен и завършен вид, обхващайки „истината“, която произтича от източника. За да обсъдим някои примери затова как прилагаме и спазваме принципа за Цялостност, можем да започнем с това, че Цялостността като принцип ни позволява да правим проверка на данните, които преминават през мрежата и по-

специално да проверяваме пакетите за грешки, като използваме метода на Проверка на Цикличния Остатък (ПЦО; от англ. Cyclical Redundancy Check (CRC)). CRC проверката е функция за сегментиране, която установява случайни промени в първични компютърни данни, които предимно се използват в цифровите телекомуникационни мрежи [20]. Ако са налице грешки, тогава информацията се препраща и проверява отново и отново. Друг пример са Електронните Подписи; криптографски алгоритъм гарантира, че човекът, който изпраща информацията е този, който се представя като изпращач. Друг такъв пример Криптографските Алгоритми за Хеширане като MD5 or SHA1. Те сравняват файла, който е действително изтеглен, като например софтуер, с първоначално избрания за изтегляне, чрез създаване на хеш стойност с фиксирана дължина, така наречен „digest“. В този случай дори една малка промяна във файла ще доведе до огромна промяна в крайния резултат (digest).

Един пример са атаките „phpMyAdmin“.При тях атакуващият може да успее да замени някои от бинарните файлове на този широко използван софтуер, като по този начин предотврати успешното провеждане на хеширани и криптографски проверки.

Цялостността и точността са наистина важни принципи, които следва да се спазват. Ако не можем да удостоверим, че съобщението, което получаваме е „надеждно“, тогава какъв е смисълът от получаването му? Представете си да гледате видео или филм с изопачена информация. Ще можете ли в такъв случай да използвате по-нататък това знание, ще се счита ли то за пълно или в случая ще сте изпуснали част от информацията?

Годност

Принципът на годност определя, че информационна система или системен източник т.е. информация остава достъпна и използваема при поискване от оторизирана системна единица, например потребител, в зависимост от спецификациите за производителност на системата. Така една система се счита за годна, ако предоставя услуги според своето устройство, както по искане конкретно искане на потребител, така и по непрекъснат, продължителен начин.

Казано по друг начин, системите трябва да са годни да функционират, а данните следва да са достъпни по всяко време, когато е нужен достъп до тях. Представете си случай, при който компютърът се изключва докато потребителят върши някаква важна работа на него или пък компютърен вирус унищожава цялата компютърна система. Подобна ситуация може да се окаже дори на живот и смърт, ако например се касае за достъп до медицинското досие на пациент, който се нужда от спешна помощ.

А какво да кажем за случаите, при които устройствата са напълно унищожени и не само услугите са недостъпни, ами всички данни са загубени? Имате ли тяхно копие, за да ги възстановите възможно най-бързо и ще се възстанови ли тяхната годност по този начин? А какво ще правите в случай, че резервните копия на данните се съхраняват на същия физически носител като оригинала им, и всички бъдат унищожени при пожар? Нужно ли е да имате няколко различни копия, които да се съхраняват на различни места?

Някои от начините, чрез които можем да осигурим по-добри и по-подходящи копия с цел да се повиши годността на данните, включват: въвеждането на “*RAID levels*“ (Резервен Масив от Независими Дискове), което представлява групирани данни на различни нива в сървърни центрове за данни, в зависимост от това доколко е нужно тези данни да бъдат годни, „*server clustering“* представлява съществуването на различни центрове за данни, но всички от тях да предоставят данни на един и същи уебсайт, като потребителят няма и представа за това, както и „*load balancers“,* които съхраняват данните на потребителите на достъпни сървъри, в случай например, че един от тях се срине.

Пример за такава атака срещу компютърна система, която води до накърняване на принципа за Годност, е DOS атаката (атака за отказ/блокиране на услуга). Атаката за отказ от услуга (DoS атака) е кибератака, при която атакуващият цели да направи определена машина или мрежа недостъпна, за да може никой от потребителите им да не може да ги използва. Тази атака може да попречи на използването на определена услуга от потребителите ѝ, тъй като на практика в този случай сървърът е „свален“ и не може да бъде използван нормално от клиентите на услугата.

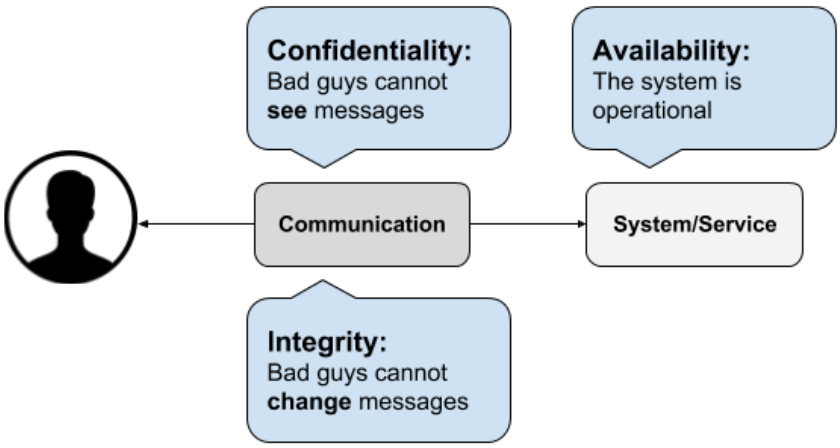
DoS атаката се извършва чрез натоварване на избраната машина или мрежа с огромен брой искания, като целта е последните да се претоварят и това да доведе до пълно или частично отхвърляне и неполучаване на някои изпратени искания.

За разлика от тези атаки, при координираните атаки за блокиране на услуги (DDoS атака) входящият трафик, който претоварва атакуваната система, произтича от много различни източници. Особеното на тази атака е, че е невъзможно тя да бъде спряна, тъй като за спирането ѝ е нужно да се блокира достъпът на всяко лице, което атакува системата.

DoS или DDoS атаките могат да бъдат оприличени на тълпа, която се опитва да мине през входната врата на магазин, като по този начин не позволяват на легитимните потребители да влязат в него. Такъв вид атака може да доведе до нарушаване на процеса на работа и извършването на операции в магазина или в съответната фирма. Атакуващите, които използват метода DoS, често насочват атаките си към сайтове или услуги, които се поддържат от уеб сървъри на авторитетни институции като банки или портали за разплащателни услуги с кредитни карти.

По-долу може да видите графично представен пример затова как трите принципа, които обсъждахме, оказват влияние върху комуникацията между системата и потребителя, както и цялостното им значение във връзка с поддържането на сигурна комуникация.

Нека предположим, че потребителят иска да се свърже със система или услуга чрез Интернет. Това може да бъде вашият клиент, който поддържа кореспонденция с онлайн магазина ви. Потребителят иска услугата да му бъде предоставяна коректно, без с нея да възникват проблеми, които могат да причинят смущения в нейната функционалност. Потребителят иска да може тайно да изпраща съобщения до системата/услугата, като не се притеснява дали тези съобщения няма да бъдат прочетени от неоторизирани лица (конфиденциалност). Заедно с това, никой не трябва да има възможност да промени тези съобщения по какъвто и да е начин чрез заместване на първоначалните данни, които потребителят изпраща [Фигура 3].



Фигура 3, основана на [6]

III. Риск

Рискът във вашата система може да бъде измерен по вероятността от неспазване на един от трите горепосочени принципа за сигурност на ЦРУ. Не си мислете, че понятието риск се отнася само за големи заплахи или атаки. Риск съществува навсякъде, дори и в най-простото нещо.

Рисковете се разглеждат по-подобно в Глава V.

IV. Общ преглед на видовете атаки

Малуер

Терминът „малуер“ (malware) е съчетание от думите “malicious software”, на български „злонамерен софтуер“. Иначе казано, малуер е всякакъв вид софтуер, който е създаден, за да причини вреди на данни, устройства или хора. Такъв софтуер се създава и разработва с цел да унищожава данни, да повлиява работата на компютъра, да предизвиква срив в системите, както и за шпиониране и разкриване на лична информация.

Исторически погледнато малуерът се е разпространявал сред потребителите чрез прикачени файлове към имейли. В имейла, получен от потребителя,

последният се моли да кликне върху прикачения файл, а със самия клик се активира и малуерът, чиято единствена цел е да причини вреди на съответната система. [7].

Всички видове малуер действат по различен начин, за да заразят и да причинят вреда на компютрите и данните в тях, поради което и всеки от тях се нуждае от различен метод, по който да се премахне. Най-доброто нещо, което може да направите, е да използвате антивирусна програма, която да включва инструменти за премахване на такъв зловреден софтуер. Освен това, не забравяйте да сте бдителни и да избягвате отварянето на съмнителни имейли и линкове [17].

Някои добре познати видове малуер са вирусите, троянските коне, шпионски софтуери, червеи, софтуер за изнудване, рекламен софтуер и ботнети. Ето и тяхно кратко описание:

Вирусът, както става ясно и от името му, се прикрепва към „чисти“ файлове и компютърни системи. Размножаването на вируси може да бъде неконтролируемо, като вредата от такава инфекция може да е значителна или дори непоправима – нарушаване на функционалността на системното ядро, унищожаване и изтриване на файлове и други. Вирусите обикновено са във формата на инсталационни файлове и се активират когато бъдат задействани (чрез кликване върху тях) [7], [17].

Троянският кон, от друг страна, се маскира като стандартен софтуер или е включен в такъв, който обаче е бил фалшифициран. Както се предполага от името му, той действа скришно и създава задни врати в системата за сигурност, за да може след това друг малуер да се внедри в нея [17].

Шпионският софтуер е вид злонамерен софтуер, който е създаден, за да следи вашата информация. Той почти винаги е внедрен в някакъв безплатен софтуер и доста често е „цената, която трябва да платите“, за да използвате последния. Това може да предизвика незначителни неприятности като наличие на изскачащи реклами или промяна на настройки без съгласие и действие от потребителя, но може и да има значително негативно въздействие върху работата на съответната компютърна система, като например да доведе до

забавяне на нейното работно представяне. Шпионският софтуер може също така да се крие в периферните слоеве на системата и да записва вашите онлайн дейности, включително вашите пароли, номера на кредитни карти, навици при онлайн сърфиране, лична или финансова информация и други. Нещо повече, този софтуер може дистанционно да поеме контрол над компютъра ви и да получи достъп до определени файлове и данни, да инсталира допълнителен софтуер или да използва компютъра ви, за да разпространява вируси [7], [17].

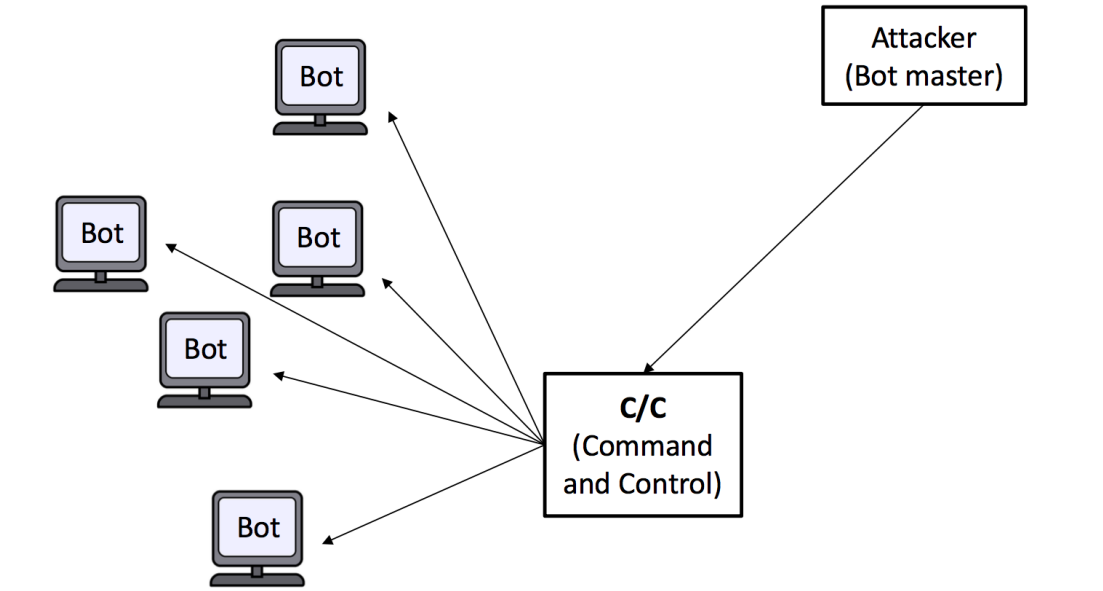
***Червеи*:** Червеят е вид вирус, който обаче се различава от другите вируси по това, че има способността да се разпространява автоматично и без човешка намеса (докато обикновеният вирус се разпространява посредством човешка дейност, например чрез отваряне на инсталационен файл). Червеят може да се разпространява от компютър на компютър като се възползва от слабостите на софтуера и хардуера, използвайки всяка следваща машина да заразява още такива [17], [18].

***Софтуер за изнудване*:** Софтуерът за изнудване е вид злонамерен софтуер, който получава достъп до вашите компютърни системи и криптира вашите файлове. По този начин той държи файловете ви като “заложници”, заедно с цялата ви система или устройство, като блокира достъпа ви до тях докато не платите откуп, в замяна на който ще получите ключът за декриптиране на файловете си [4]. Софтуерът за изнудване е обяснен по-подробно в следващите подтеми.

***Рекламен софтуер*:** Рекламният софтуер не е директна заплаха за компютърните системи както другите малуери (злонамерени софтуери), тъй като е софтуер за рекламиране на определени продукти. Проблемът при него е, че той може да подкопае вашата сигурност, за да постигне целите си, като такава цел може да бъде и внедряването на друг вид малуер във вашата система [17].

***Ботнет атаки*:** Атакуващите обикновено се опитват да компрометират сървъри, които съдържат ценна информация относно определена фирма или нейните потребители. Един от начините да се навреди на такъв компрометиран сървър е чрез контролиране на няколко обикновени хостове (т.е. компютри) като ботове. Тези ботове могат да обхващат Ботнет (като армия от компрометирани машини, виж Фигура 4) [6], която може да бъде използвана по много различни

начини за атакуване на други хостове, като същевременно се запазва анонимността на атакуващия.



Фигура 4

Ботнет в общи линии представлява голям брой компрометирани хостове, които се контролират от атакуващ, наречен Бот Мастър (Господар на ботовете [англ.] – бел. пр.). Тези мрежи често са използвани посредством наемане за всякакъв вид злонамерени дейности. Така например, някой може да намери такъв Бот Мастър и да поиска от него да използва своите Ботнети, които да кликват на измамни линкове с цел генериране на печалба или трафик, да изпращат СПАМ имейли до много различни потребители, да събират фалшиви лайкове във Фейсбук/Туитър или да публикуват вече публикувани постове. Една от най-честите цели на атакуващ, който е наел Ботнет от Бот Мастър, е извършване на Атака за отказ/блокиране на услуга (DDoS) срещу конкретно посочен хост.

В този случай Бот Мастъра контролира Ботнетите чрез скрити команди и канал за управление (BotNet C/C). Ботовете периодично проверяват този канал, за да получат нови команди, като тези команди често идват от публичното пространство, виж Фигура 5 [6]. Пример за това е използването на туитър акаунт, който е създаден точно за такъв вид атаки. Атакуващият туитва криптирана команда, така че никой да не може да разбере каква е самата команда. BotNet

C/C (ботнет компютрите) обаче могат да декриптират и изпълнят командата, използвайки ключ от атакуващия.

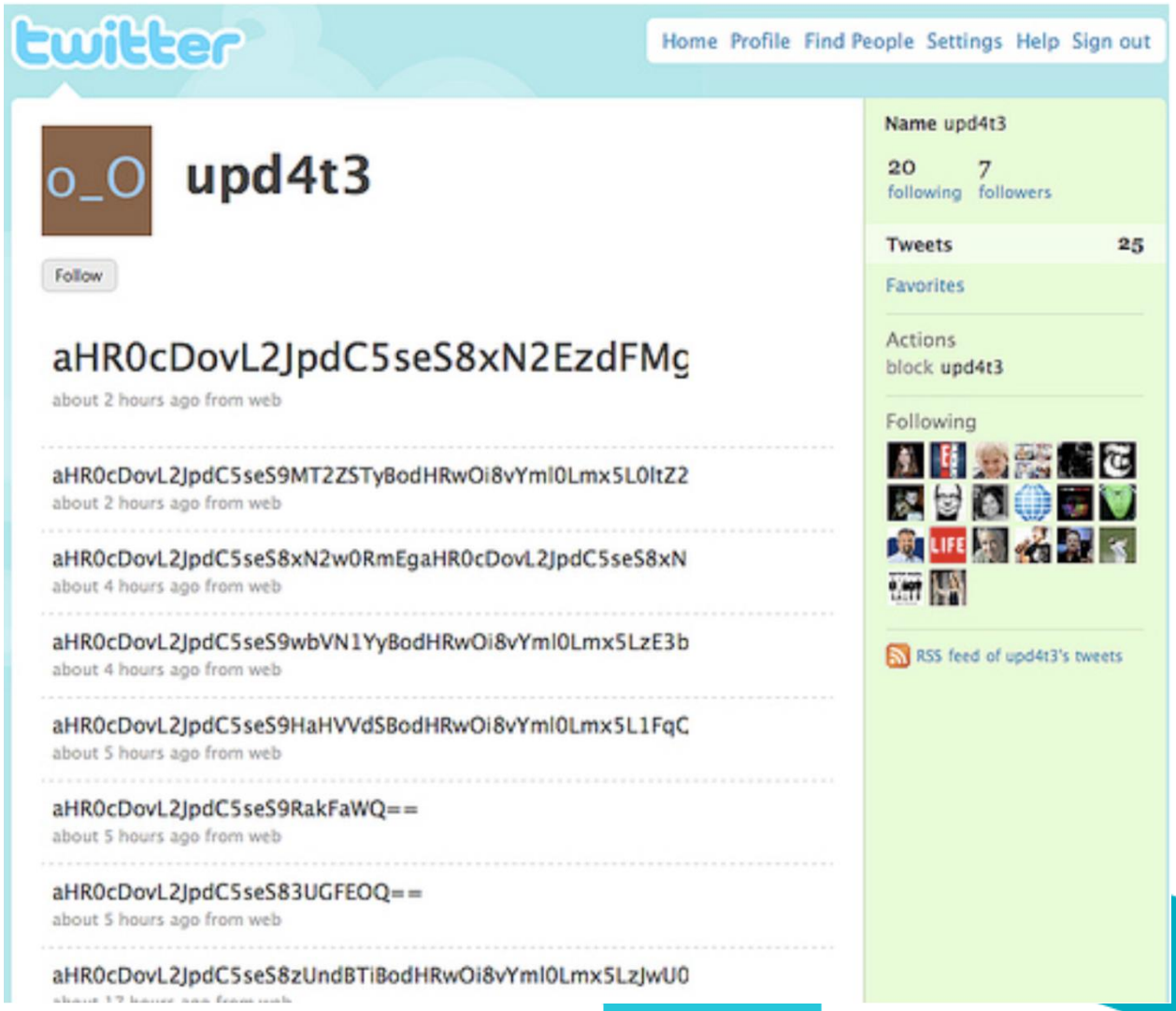


Figure 5

<u>Нека разгледаме няколко известни примери за горепосоченото:</u>

През 2000-та година вирусът “ILOVEYOU”(“Обичам те” [англ.] – бел.пр.) предизвика най-опустошителната малуер атака за всички времена. Вирусът идва с имейл, в заглавието на който пише “Обичам те”. Това, което прави “ILOVEYOU”, е да презаписва личните файлове на съответната система и да се разпространява отново и отново [24].

“Storm Worm” вирусът пък е Троянски кон, който заразява компютрите, като понякога ги превръща в зомбита или ботове, за да продължат да разпространяват вируса и да изпращат огромни количества от спам имейли.

Устройствата се заразяват, когато хората отворят имейл, който гласи “230 загинали, буря удари Европа” и кликнат върху линка, като до юли 2007 година „Storm Worm“ е засечен в над 20 милиона имейла [24].

Друг много известен пример за Софтуер за изнудване е „CryptoLocker“, който е пуснат през септември 2013 и се разпространява чрез прикачени към имейли файлове, като криптира файловете на потребителите и последните нямат достъп до тях [24].

Уеб-базирани атаки

Уеб-базирани атаки са тези, които използват включените уеб системи и услуги, включително: браузъри (заедно с техните разширения), уебсайтове (включително CMS - Content Management Systems [Системи за управление на съдържанието – бел.пр.]), както и ИТ компоненти на уеб услуги и приложения.

Съществуват различни видове такива атаки, като например:

- използващи уеб браузъра (или негови разширения),
- използващи уеб сървъри или услуги,
- съпровождащи атаки,
- water-holing атаки,
- пренасочващи и man-in-the-browser атаки.

Използващите уеб браузър атаки са форма на злонамерен код, който използва уязвимостите в оперираща система или в инсталиран софтуер, като целта е да се пробие сигурността на браузър потребителските настройки на последния, без обаче самите потребители да знаят за това [32].

Използващите уеб сървъри и уеб услуги атаки са част от софтуер или част от данни, които се възползват от определен бъг или уязвимост на уеб сървъра или уеб услугата, за да предизвикат нежелан или непредизвикан режим на работа. Този режим на работа може да позволи на атакуващите дистанционно да поемат контрола върху заразените уеб сървър или уеб устройство, като по този начин им позволи да се задейства и изпълни злонамерен код.

Съпровождащи са атаките, които се осъществяват чрез нежелани изтегляния на компютърен софтуер от Интернет и могат да бъдат два вида:

- изтегляния, които потребителят сам е решил да инициира, но без да разбира възможните последици, като например изтегляне, което инсталира неизвестна изпълнима програма, компонент на ActiveX или Java аплет (софтуерно приложение) автоматично,
- изтегления, които са инициирани без знанието на потребителя, като такива изтегления могат да бъдат стартирани просто от посещаването на даден уебсайт или от преглеждането на html имейл съобщение, което е с вграден зловреден код във HTTP или PHP кода [33].

Water-holing атаките са такива атаки, при които атакуващият предполага или наблюдава кои уебсайтове са често посещавани от конкретна жертва или от определена група (например организация, индустрия или регион), след което заразява един или повече от тези уебсайтове със злонамерен софтуер (малуер). A watering hole е такъв вид стратегия за компютърна атака, при която жертвата е определена група потребители, като с тази атака могат да се заразят членовете на таргетираната група чрез специфични конфигурации на злонамерения софтуер, така че да могат да се разграничат потребителите, които са целта на атаката от заразените такива. [34]

Пренасочването на потребители от легитимен уебсайт към друг уебсайт е възможно чрез въвеждането на злонамерен код в конфигурационния файл на определен уеб сървър. След това атакуващият иска от потребителите да въведат своя чувствителна информация в злонамерен сайт, като обаче изглежда, че те са пренасочени в надежден уебсайт. Man-in-the-browser-атаките са създадени така, че да прихващат данни, които преминават през защитена комуникация между потребител и онлайн приложение [35].

Атаки чрез уеб приложения

Атаките чрез уеб приложения са насочени срещу достъпни уеб приложения, уеб услуги, както и срещу мобилни приложения. Такива атаки опитват да злоупотребят с ППИ (приложни програмни интерфейси), които са част от уеб приложения. Атаките чрез уеб приложения обикновено са насочени към добре познати източници и проекти, които са базирани на отворен или обществено

достъпен код, като например приставки за Joomla и Wordpress, сайтове на Magento и други.

Тези видове атаки чрез уеб приложения могат да бъдат изброени, както следва:

- SQL Injection (SQLi) attacks,
- Local File Inclusion (LFI),
- Remote File inclusion (RFI),
- Cross-site Scripting (XSS),
- PHP injection (PHPi) or PHP Object Injection [36].

SQL Injection (SQLi) атаките представляват техника за инжектиране на код. Те се използват с цел атакуването на управлявани от данни приложения, при които фалшиви SQL заявки се добавят във входното поле за изпълнение. SQL Injection е една от най-критичните уязвимости на системите, като такъв вид атака позволява да се получи достъп до различни данни, включително: имена, номера на кредитни карти и всякакъв друг вид конфиденциални и чувствителни търговски данни [37].

Local File Inclusion (LFI) е прикриваща атака, при която атакуващият може да заблуди уеб приложението да включи файлове на уеб сървъра с помощта на използването на функционалност, чрез която динамично се включват локални файлове или кодове. Последицата от такава атака може да се изрази в: Directory Traversal and Information Disclosure (Разместване на директории и разкриване на информация) или дори Remote Code Execution (Дистанционно изпълнение на кода). Local File Inclusion е много сходна атака с Remote File Inclusion (RFI) атаката.

При RFI атаките атакуващият, в сравнение с LFI атаките, може не само да включи локални файлове, но също така и отдалечени файлове [38].

Cross-site Scripting (XSS) са вид атаки с инжектиране на клиентски код, при които атакуващият може да приложи злонамерен код към надежден сайт или приложение [39].

PHP injection (PHPi) or PHP Object Injection уязвимост в нивото на сигурност на приложение, което позволява на атакуващия да извърши различни видове

злонамерени атаки, като например: SQL Injection, Application Denial of Service, Code Injection и Path Traversal според контекста [40].

Атака за отказ на услуга

DoS атаката (атака за отказ/блокиране на услуга) е такава атака, която цели да се изключи определена машина или мрежа, като по този начин последната се направи недостъпна за потребителите. Атаките за отказ на услуга обикновено се осъществяват чрез насочването на голям трафик на данни или изпращането на информация, която предизвиква срив в съответната система. Независимо за кой от двата случая се касае, DoS атаките препятстват достъпа на служители, притежатели на профили, както и на всички други действителни потребители, до определената услуга или система. Банки, търговци, медийни компании и правителствени организации, както и други авторитетни организации са обичайните жертви на атаките за отказ на услуга. Тези атаки в общия случай не водят до кражба или загуба на информация, или до загуба на други ценни активи, но отнемат значително време и усилия, за да могат компаниите да се справят с тях. Друг тип DoS атака е Координираната атака за отказ (блокиране) на услуга (DDoS). Координираната атака за отказ на услуга се осъществява с помощта на множество системи, като последните извършват синхронизирана DoS атака. Разликата в двете атаки се състои в това, че при DDoS атаките целта се атакува от много различни адреси едновременно [41].

Спам

Спамът сам по себе си е стар колкото самия Интернет, но въпреки това остава един от основните начини за заразяване с малуер, като за целта се използват злонамерени прикачени файлове и линкове. Спамът представлява над 85 процента от всички изпращани имейли, а спам акаунтите заемат повече от 50 процента от всички имейл адреси по света. Спам имейлите се изпращат от големи групи от ботнети или заразени с вируси компютри и могат да бъдат представени като канали за рекламиране на лекарствени продукти, еротични услуги или онлайн запознанства. При тези атаки е важно потребителите да се запитат дали познават този, който изпращаща имейла, преди да го отворят,

както и дали съдържанието и формата на прикачените файлове е вярно, ако познават изпращача на съответния имейл [42].

Фишинг

Фишингът използва предимно някои техники за социално инженерство, за да атакува крайните потребители. Тези техники се използват с цел заблуждаване на потребителите и използване на техните слабости по отношение на уеб сигурността им. Фишинг атаките обикновено се извършват чрез злонамерен имейл, получен от потребителите, в който биват убеждавани да посетят измамен уебсайт, който от своя страна се опитва да получи достъп до тяхна чувствителна информация като потребителски имена, пароли и информация за кредитните им карти, които данни да се използват недобросъвестно. Във фишинг имейл може да твърди например, че последният е изпратен от вашия банков асистент, който любезно ви моли да му предоставите вашите удостоверяващи данни за онлайн банкирането си, за да може той да ви помогне с разрешаването на определен ваш проблем, може изпращачите да се представят за доброволци от Червения Кръст, които ви молят да предоставите номера на кредитната си карта, за да могат да приемат вашето дарение за хората в нужда и така нататък. Поради това трябва да бъдете много внимателни и да търсите логиката във всичко, като имате предвид, че такива организации никога не биха поискали да им предоставите вашите идентификационни данни посредством имейл. Не всички хора и организации са добросъвестни, така че винаги имайте едно наум. Съществува голяма вероятност това всъщност да е атакуващ, който се опитва да открадне ценна информация от вас.

Фишинг механизмите също така стават все по-целенасочени и все повече се усложняват, което прави засичането на фишинг атаките изключително трудно. Вече често се използват и моменти съобщения, а не само имейли.

Фишинг атака може да се осъществи и чрез фалшив уебсайт, който много прилича на някои популярни сайтове. Важно е да се подчертае, че тези измамни уебсайтове обикновено изглеждат по същия начин като действителните такива, а единствената разлика между двата се състои в URL адресите им. Например, по някакъв начин някой успява да ви пренасочи към сайт, наречен

www.bankofvvest.com вместо www.bankofwest.com. Двата сайта много си приличат, но първият е фалшив уебсайт, който се контролира от атакуващия и целта му е последният да се добере до вашите лични данни, включително до банковите ви сметки, кредитните ви карти, както и друга чувствителна информация. Последният даден пример може да бъде избегнат с правилното използване на определени сертификати, на които ще обърнем специално внимание в друга част на ръководството. Казано най-общо, фишинг кампаниите са се повиши както по своя обем, така и по сложността си. Фишингът обикновено се използва като първата стъпка при осъществяването на кибер атаки, като поради тази причина той се свързва с повечето от заплахите за дигиталната сигурност в наши дни, като например: ботнети, малауер, web-based атаки, exploit kits, кибер шпионаж и други. [43]

Вътрешна заплаха

Вътрешната заплаха, както може да се заключи от определението ѝ, представлява такава заплаха, при която вътрешен потребител използва своя оторизиран достъп, преднамерено или случайно, за да се предизвика пробив в сигурността. Следва да се отбележи, че тези вътрешни заплахи представляват огромен риск за значителен брой институции и организации, без значение от местоположението, големината или областта, в която действат последните. В подобни ситуации се оказва изключително трудно за повечето организации да разграничат тези вътрешни заплахи от нормалната дейност на служителите им, която не носи опасност. Инцидентите, причинени вследствие на потребители с оторизиран достъп, могат да бъдат умишлени или поради недоглеждане. Важно е да споменем, че загубите, причинени вследствие на вътрешна заплаха, често остават неразкрити. Въпреки това, привилегированите потребители, включително мениджърите с достъп до чувствителна информация, са тези, които представляват най-голяма заплаха за организациите [44].

Кражба на самоличност

Кражбата на самоличност се явява като специален случай на пробив в сигурността. Тази атака цели да получи достъп до конфиденциална информация, която може да бъде използвана, за да се установи самоличността на човек или

дори да се установи определена компютърна система. При този вид атака, атакуващите целят да получат достъп до: подлежащи на идентификация имена, адреси, данни за връзка, документи, данни за финансовото и здравословното състояние, акаунти и други данни. Щом веднъж атакуващият притежава личната информация на жертвата, той може да източи банковите ѝ сметки, да натрупа задължения по кредитните ѝ карти, да открие нови сметки на нейно име или дори да получи медицинско лечение по здравната застраховка на жертвата. Нещо повече, той може дори да се представи с името на жертвата, ако от полицията го задържат. Според Федералната комисия за търговия, независима агенция към правителството на САЩ, кражбите на самоличност могат да се класифицират в 6 отделни категории: свързани с назначаване на работа или данъчни измами (използвайки информацията на някой друг, за да се получи назначение на работа или за подаване на данъчна декларация), измами с кредитни карти (използване на нечия друга кредитна карта или номер на такава, за да се правят измамни покупки), телефонни измами или такива, свързани с ползването на услуги (откриване на сметка за телефон или за друга услуга чрез използването на личната информация на друг човек), банкови измами (чрез използване на личната информация на друг човек, за да се поеме контрол над неговата сметка в банката или пък да се открие сметка на името на човек, който дори не подозира), измами със заеми или наеми (използване на нечия чужда самоличност за изтеглянето на заем или наемането на нещо), измами с правителствени документи или с държавни помощи (използване на крадена информация с цел получаване на държавни помощи) [45].

Теч на информация

Течовете на информация са сериозно заплаха за киберсигурността в наши дни. Тези течове представляват различни видове пробиви в достъпа до информация, които варират от събирането на данни от Интернет гиганти и онлайн услуги до съхраняването на търговски данни в инфраструктурните обекти на ИТ компании [46].

Кибер-шпионаж

Кибер-шпионажът представлява кражба на тайни и информация, която се съхранява на дигитални формати или на компютри и ИТ мрежи, без позволението и знанието на притежателя на информацията, от лица, които са конкуренти, врагове определени групи или държавни структури, като целта на тези кражби е получаването на лично, икономическо, политическо или военно превъзходство. Кибер-шпионажът обичайно включва използването на такава тайна информация или контролирането на определени компютри / цели мрежи, чрез които да се постигне стратегическо и психологическо предимство, политически дейности и саботаж. Отскоро кибер-шпионажът включва също и анализ на публични дейности в социалните мрежи, включително Фейсбук и Туитър [47]. Интересно е да се отбележи, че в повечето случаи потребителите или организациите, чиято дигитална сигурност е компрометирана, дори не са наясно с това. Но кои са най-добрите средства за защита от техническите рискове във връзка с дигиталната сигурност, като например: малуер (злонамерен софтуер), уеб-базирани атаки, атаки чрез уеб приложения, фишинг, спам, блокиране услуги, софтуер за изнудване, ботнети, вътрешни заплахи, физическо манипулиране, пробиви в сигурността, кражба на самоличност, теч на информация, exploit kits, кибер-шпионаж. Казано просто, прилагането на предпазни мерки при използване на Интернет и други нови технологии е в състояние да предотврати излагането на горепосочените технически рискове. Операционната система на компютъра трябва да бъде актуализирана възможно най-рано (могат да се приложат автоматични актуализации), тъй като хакерите често използват известни пропуски в сигурността на операционните системи за постигане на техните цели. Своевременните актуализации често са от голямо значение за работата на различните приложения на компютри, смартфони, таблети или дори на Интернет устройства, като щом определен пропуск бъде намерен и обявен от софтуерните компании, хакерите започват да създават програми с цел недобросъвестното използване на тези пропуски. Уеб приложения, уеб услуги, уебсайтове (включително CMS – „Content Management Systems“, в превод Системи за управление на съдържанието), следва също да бъдат обновявани редовно. Браузъри и приставки също трябва да се

актуализират до най-новите им версии, а потребителите не бива да теглят прикачени файлове или да кликват върху линкове в имейли, които изглеждат подозрително или пък са им непознати. Софтуерът Firewall (в превод „защитна стена“) и Интернет защитните мерки, както и антивирусните програми следва да се използват и обновяват редовно, особено когато потребителят сърфира в Интернет. Подозрителни сайтове не трябва да се посещават, а използваните пароли не трябва да бъдат лесни за отгатване (с ниско ниво на сигурност) и е добре те да се сменят често (специалистите съветват на всеки 4 седмици). Редовният бек-ъп на данните и съхранението им на сигурни места също е препоръчително. ИТ администраторите следва да осигуряват коригирането и обновяването на всички системи в мрежата. Лицата трябва да бъдат внимателни при споделянето в социалните мрежи, като е важно да не се посочват много лични детайли в техните профили [48].

V. Други потенциални проблеми за бизнеса

Различните заплахи постоянно се увеличават, опитвайки се да измамят хората чрез използването на нови несъмнено изобретателни начини. Такива начини са:

- Измамни телефонни обаждания, които действат по подобие на фишинг имейлите. При тях хора ви уверено твърдят, че имат нужда от определена информация от вас във връзка с определен фалшив проблем. Например те могат да ви кажат, че се обаждат от Майкрософт и че са открили наличие на вирус във вашата система. Заради това, за да могат да ви помогнат с решаването на проблема, те ще се нуждаят от вашите идентификационни данни за вход, както и от друга информация.
- Физическото присъствие на неоторизирани хора във вашето сървърно помещение, пред вашия компютър или лаптоп. Това може да е някой, който е проникнал в помещението с цел кражба на данни или дори някой, който се преструва, че е потребител, но всъщност се взира в данните на екрана ви докато вие търсите из системата и се опитвате да отговорите на въпросите му относно цените и стоката.
- Софтуерът за изнудване е наистина голяма заплаха и за малките, и за големите компании, както за прохождащия предприемач, така и за

огромното предприятие. Това е атака, при която агент получава достъп до компютър, криптира всички данни в него по такъв начин, че последните да не могат да бъдат използвани повече, след което изнудва потребителят за откуп, за да декриптира информацията му. Детайлен пример затова ще бъде даден в следващите два раздела.

- На последно място, но не и по значение, все по-интелигентни и приспособими вируси и друг малуер се проявяват като ежедневна заплаха за компютърните системи. Поради това инвестирането в надеждна антивирусна програма, която постоянно актуализира своята база данни от вируси, може да бъде много ефективно и целесъобразно решение, което да отговори на вашите потребности.

L. Влияние на пробивите в дигиталната сигурност върху процесите в бизнес средата (търговията)

I. Влияние

Вече описахме горепосочените случаи, при които наличието на технически пробив в бизнес компютърна система, породен от липсата на достатъчна сигурност, може да доведе до смущаване на бизнес процесите. По един или друг начин, ако системата или част от нея се срине, това означава големи загуби за бизнеса. Тези загуби не винаги са финансови, те могат да се изразяват в загуба на време или усилия, загуба на бъдещи или потенциални клиенти, ценна информация или дори завеждане на съдебно дело.

От най-обикновеното нещо като разпадане на интернет връзката за няколко минути до най-сериозните случаи като кражба на информация за клиентите, лоши неща се случват постоянно.

Пропускане на краен срок, невъзможност за издаване на фактури или разписки, за извършване на транзакция или продажба, както и за извършване на доставка навреме, публично излагане на чувствителна информация и злоупотреба с нея, загуба на цялата информация относно даден акаунт и кражба на данните на вашия администратор, са само част от ситуациите, с които предприемачите могат да се сблъскат, поради неадекватна защитна конфигурация на тяхната система.

А какво бихте направили, ако някой открадне вашите данни, влезе с тях във вашия онлайн магазин и започне да го контролира? В такъв случай вие може да изгубите целия си бизнес, ако нямате резервен план за действие.

Както вече споменахме, атаката със *софтуер за изнудване* представлява много сериозна ситуация. Нека използваме този пример като ***казус,*** който ще изследваме в тази глава.

II. Казус за изследване: Софтуер за изнудване

Софтуерът за изнудване е такъв тип злонамерен софтуер, който получава достъп до вашите компютърни системи и чрез криптиране на файловете ви държи последните, а и цялата ви система като „заложници“, като блокира достъпа ви до тях докато не платите желания откуп, в замяна на който ви предоставя ключът за декриптиране на файловете. Както подробно обяснихме в предишната глава, криптираните данни са невъзможни за разчитане в случай, че не притежавате ключа за декриптиране [4]. Разбира се, дори ако платите откупа, никой не може да ви гарантира, че ключът за декриптиране ще ви бъде даден. Не забравяйте, че си имате работа с престъпници, които се интересуват единствено от парите ви, не и от вашата информация. Ако поискат вашите банкови данни или данните на кредитната ви карта и вие им ги предоставите, те може би ще се опитат да увеличат дори още печалбата си, използвайки тази информация понякога дори след като са ви пратили ключа за декриптиране (ако изобщо ви го пратят). Те могат също така да ви пратят файл за “отключване”, който допълнително да зарази вашия компютър със злонамерен софтуер [28].

Човек може да се „сдобие“ с такъв софтуер за изнудване чрез прикачен в имейл файл, изтеглен злонамерен файл, хакнат уебсайт или привидно безобидна, но в действителност злонамерена реклама. Използването на нелицензиран софтуер, P2P Мрежи или заразено със софтуер за изнудване USB могат потенциално да заразят вашето устройство [29]. Щом веднъж сте заразени със софтуер за изнудване, вие ще забележите, че вашите файлове, изображения и данни изобщо са били криптирани и не можете да ги отворите. В същото време най-вероятно ще ви се покаже изскачащ прозорец, в който ще искат да платите откупа, а след това ще ви уведомят какво ще се случи, ако него направите.

Атаките чрез софтуер за изнудване са познати от десетилетия, но все още са едни от най-големите заплахи, пред които бизнесът и отделните лица могат да бъдат изправени в наши дни. Тъй като вече съществуват методи за предотвратяването на такива атаки, техните разновидности се развиват и се подобряват начините им на разпространение, затруднява се откриването им, усложнява се процесът на криптиране, което принуждава потребителите да плащат исканите им откупи. Всеки такъв нов софтуер е все по-сложен и създава

все повече трудности във връзка с предотвратяването на действията му, като нанася и все по-осезаеми вреди на жертвите си.

Исторически факт е, че първият софтуер за изнудване, който познаваме, е пуснат през 1989 година и неговата цел е била здравната индустрия, която между впрочем и до ден днешен е една от основните цели на такива атаки. Благодарение на някои ловки киберпрестъпници, използването на софтуер за изнудване се превърна в доста доходоносен бизнес, като последните започнаха да предлагат софтуер за изнудване под формата на програма за услуги. Някои от най-разпространените софтуери за изнудване са CryptoLocker, CryptoWall, Locky и TeslaCrypt. От тях само CryptoWall успя да генерира повече от 320 милиона долара приходи .

Обичайните суми, които се искат за откуп в наши дни варират около 500 долара. Обикновено на жертвата се дава краен срок да плати откупа, като му се казва, че ако не го спази, то искането ще се увеличи двойно или файловете му ще останат напълно недостъпни за него, ще бъдат унищожени или ще бъдат изложени публично.

Следователно, очевидно е, че атаките чрез софтуер за изнудване могат да донесат значителни негативни последици на бизнеса, независимо дали става въпрос за бизнес на млад предприемач или за предприятието на вече развита компания. Годността се превръща в сериозен проблем и ако не сте подготвени да се приведете в съответствие с този принцип, тогава най-вероятно ще претърпите загуба на данни или на пари, заедно с всички произтичащи последици от това.

В случай, че се интересувате от темата, можете да прочетете и да се запознаете с детайлите около най-големите 10 атаки чрез използване на софтуер за изнудване за 2017 година [9].

В края на следващия раздел ще обсъдим действията, които могат да се предприемат с цел да се предотвратяват подобни атаки, причинени от софтуер за изнудване.

M. Разрешения във връзка с Киберсигурността

I. Рамки за сигурност

Осигуряването на защитни механизми за вашите компютърни системи често може да се окаже доста странно и объркващо нещо. За да улесните задачата си, вие можете да използвате такива ръководства като Рамки за Сигурност и стандарти, в които се обяснява как да постигнете определено ниво на сигурност, както и кои действия трябва да се избягват. Иначе казано, чрез следването и изпълняването на тези ръководства вие ще можете да затвърдите и да повишите нивото на вашата сигурност. Все повече рамки за сигурност могат да бъдат приложени в почти всички видове търговска дейност, като последните са в състояние да изберат кои насоки от тях да спазват. Като примери за такива рамки за сигурност можем да посочим NIST Frameworks [25], ISO Frameworks [26] и CIS Framework [27].

Когато се колебаете коя рамка за сигурност да приложите, изберете тази, която е сравнително лесна за следване и изглежда подходяща за вашия случай. Щом веднъж изберете рамка, след това трябва да решите кои нейни механизми са най-релевантни за вашия бизнес. В зависимост от процесите, които се извършват във вашия бизнес и нуждите на последния, може да не е наложително да сте в съответствие с всичко или да приложите всички възможни мерки от самото начало. Благодарение на това вие всъщност създавате своя собствена рамка за политика на сигурност, която да следвате и съответно да доразвиете с течение на времето.

II. Други мерки по отношение на сигурността

В предишните глави разгледахме значителен брой такива мерки, който бяха предимно посочени като примери. В обобщение, някои мерки могат да осигурят разрешения във връзка със заплахите за Киберсигурността, като такива са:

- Цялостните и редовни копия на цялата информация;
- Инсталиране на антивирусна програма и друг защитен софтуер, които да са подходящо настроени за различните устройства. Моля, имайте

предвид, че в някои случаи е по-рентабилно да си закупите такъв лицензиран софтуер вместо да използвате безплатни или пробни версии на такива;

- Честа актуализация на вашите системи;
- Съответствие с рамката за сигурност или определени части от нея;
- Избиране на трудни за разбиване („сложни“) пароли, които не споделяте с никой и не разкривате по някакъв начин;
- Придобиване на https сертификат на вашия уебсайт;
- Недопускане на неоторизирани лица да имат физически достъп до вашите помещения или устройства;
- Използване на софтуери само от надеждни източници, които са легитимни, проверени и обхващат всички необходими технически мерки за сигурност.

Съществуват множество различни онлайн инструменти, които можете да използвате, както, за да оцените нивото на вашата сигурност, така и за да установите дали последната е била пробита.

- Инструменти за оценка на нивото на защита могат да бъдат особено полезни, за да проверите колко добре сте успели да приложите мерките за защита във вашия бизнес. Пример за такъв инструмент е Microsoft Security Assessment Tool, който може да бъде намерен и изтеглен на посочения линк [10]
- Инструменти, които ще ви помогнат да разберете за потенциални рискове за вашите имейл акаунти. Някои от тях също така подчертават сериозността на различните рискове от онлайн атаки в Интернет. Такъв пример е инструментът “Have I been pwned?”, който може да бъде намерен на долупосочената страница [11]. Всички данни, които използва този инструмент са от публично изтекли „пробиви в сигурността“ или иначе казано, това са лични данни на различни акаунти, чиято информация е била откраднатa и впоследствие е пусната в публичното пространство. “Have I been pwned?” най-просто казано събира тези данни на едно място и ги прави лесно достъпни.

III. Казус за изследване Част II

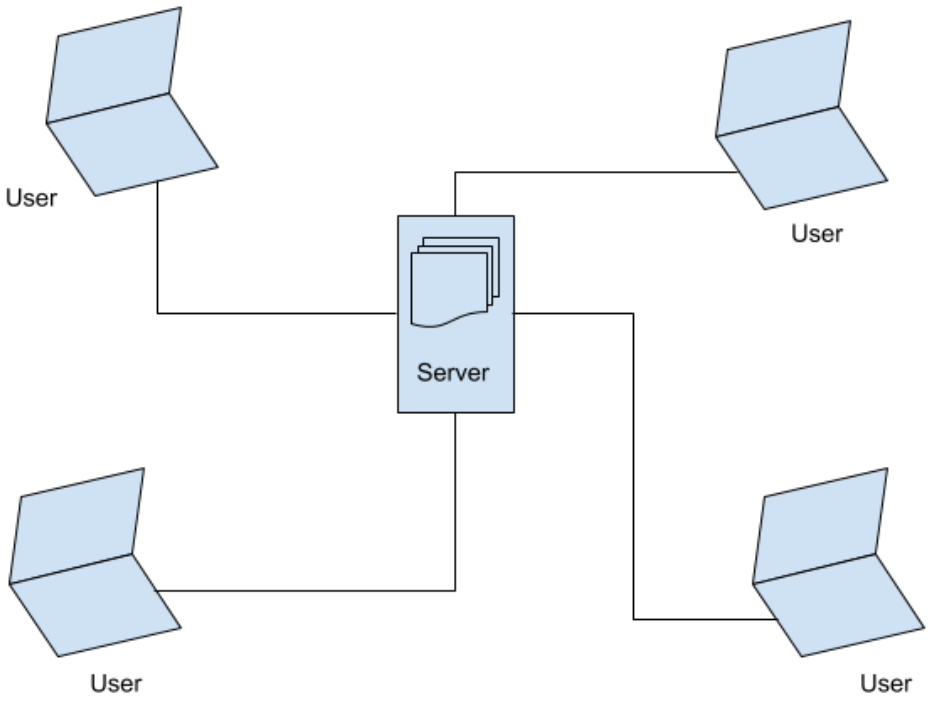
Разглеждайки отново казуса относно Софтуера за изнудване, ние можем да анализираме стъпките, които са необходими за разрешаването на този проблем.

На първо място, вие трябва да разберете, че докато осъзнаете, че сте атакуван от такъв софтуер, вашите данни (всички или някои от тях) вече ще бъдат декриптирани. Как трябва да реагирате в такъв случай?

Първата стъпка, която трябва да предприемете, е да се опитате да **спрете атаката**. За да направите успешно това, вие трябва да блокирате достъпа на заразеното устройство до мрежата. Ако в случая имате централизирана директория на файлове, тоест сървър, в който се съхраняват всичките ви документи и до който имат достъп потребители от различни устройства, то вие трябва незабавно да блокирате възможността на всички потребители да правят промени на сървъра. Това следва да бъде направено, тъй като софтуерът за изнудване действа чрез заразяване на потребителите, поради което е нужно да ограничите достъпа на заразените потребители до останалите данни на сървъра. Един от начините да постигнете това е като промените настройката на сървъра на "Само за четене", така че потребителите да не могат да правят промени на него. Това, разбира се, ще се отрази и негативно, защото ще блокирате достъпа и на всички „невинни" потребители, които също нямат да могат да правят промени на сървъра. Особено важно в случая е да не изключвате сървъра. Последният е нужно да работи, за да могат да се запазят всички скорошни влизания на потребители.

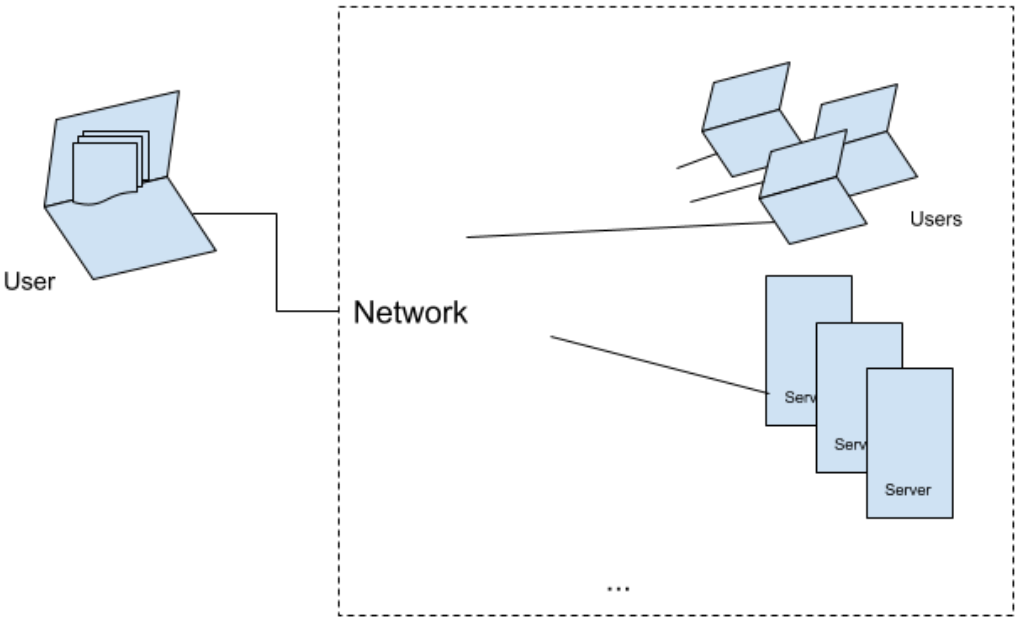
След като сте направили горепосоченото, трябва да намерите заразения потребител, за да оставите ограниченията за сървъра само по отношение на него/нея и да възстановите достъпа на останалите потребители. Заразеният потребител може да намерите като проверите кой е имал достъп до атакуваните файлове, както и кой ги е преглеждал (отварял) преди атаката. След като го намерите, трябва да инструктирате заразения потребител веднага за извади ethernet кабела, за да прекъсне връзката си с мрежата (или да прекъсне връзката с wi-fi мрежата), като по този начин окончателно ще спрете атаката. Имайте предвид, че потребителят не трябва да изключва компютъра си, защото в

неговата памет може да има особено важна информация относно атаката, която ще бъде изтрита след спиране на захранването.



Фигура 8 – Централизирана директория на файлове

Ако пък например сте единствен потребител и файловете се съхраняват на вашето устройство, изключете устройството си от мрежата, но отново не го изключвайте изцяло поради горепосочените съображения.



Фигура 9 – Съхраняване на файлове на едно устройство

Втората стъпка, която трябва да предприемете, е да **оцените пораженията,** които са нанесени. В случай, че преди атаката сте били в съответствие с принципа на Конфиденциалност, то може би нанесените вреди ще са ограничени. В случай на централизирана директория на файлове, ако всеки един от потребителите е имал достъп само до определени файлове на сървъра и атакуващият е осъществил атака си чрез един единствен потребител, тогава само неговите/нейните достъпни файлове ще бъдат засегнати. Ако пък преди атаката системата ви е била в съответствие с принципа на Цялостност, то вие ще може да проверите кои точно файлове са засегнати от атаката, като ги сравните с техни предишни версии (т.е. скорошни копия). При оценката на нанесените поражения можете също така да създадете копие на вашия диск или само на заразените файлове с цел по-нататъшното им анализиране.

Третата и финална стъпка се отнася до **Възстановяването**. Тук следва да посочим, че в разглеждания казус принципът на Годност също е нарушен

вследствие на атаката. Най-доброто, което можете да направите, е да почистите вашата система, а след това да възстановите всичките си данни с помощта на някое скорошно копие. За да почистите системата си преди да пристъпите към възстановяване на вашата информация, вие можете да форматирате или преинсталирате операционната си система или пък да „дезинфекцирате“ устройството си като го включите в безопасен режим и пуснете цялостна проверка на антивирусната програма. Това няма да ви помогне да декриптирате данните си, но може да изчисти системата ви от заразяването, така че да можете за използвате спокойно възстановените си файлове. Ето, сега вече наистина разбирате значението своевременно направените резервни копия. От всичко казано до тук излиза, че проблемът с Годността е разрешен. Само не забравяйте отново да върнете достъпа до сървъра.

В случай, че нямате направени резервни копия, ето списък с някои неща, които можете да опитате [30], [31]:

- върнете системата до безопасна точна на възстановяване, ако имате такава;
- възстановете по-стара версия на файловете, като използвате софтуер тип „shadow explorer“ или инструмент за възстановяване на данни;
- опитайте да уставите специфичния вид софтуер за изнудване (съществуват някои достъпни онлайн инструменти, с които можете да го направите) и ако успеете, проверете дали има декриптиращ инструмент за този вид софтуер, който да използвате.

Гореизложеният сценарии, макар да звучи стряскащо, може да бъде разрешен сравнително лесно, особено ако сте в съответствие с трите основни принципа на информационната сигурност и сте наясно с мерките за защита и разрешенията, които обсъдихме в този раздел .

N. Контролен списък за Киберсигурност

	✓
Компютрите редовно правят резервни копия	
Системите се обновяват редовно и своевременно	
Антивирусната програма е инсталирана правилно и работи според конкретните нужди	
Инсталирана е защитна система тип „защитна стена“	
Извършена е оценка на рисковете и наблюдение	
Прилага се рамка за сигурност, с цел да се повиши нивото на сигурност	
Създадена е VPN Мрежа за използване от потребителите ви, когато е необходимо	
Осигурете сертификат за сигурност за вашия уебсайт (Https)	
Не влизайте в сайтове, които се категоризират като несигурни от вашия браузър	
Използване на пароли с високо ниво на сигурност, които не се показват на неоторизирани лица	
Контролирайте физическия достъп до помещенията и устройствата си	

Потвърдете самоличността на изпращащия ви имейл преди да му предоставите каквито и да е данни или да кликнете върху каквито и да е файлове от имейла	
Криптиране на всички чувствителни данни, които се съхраняват (т.е. използвайки специализиран софтуер)	
Не теглете съмнителен (нелицензиран) софтуер	
Контролен списък с настройки на „Защитна стена“	
Използвайте набор от правила с разрешени услуги на вашата „Защитна стена“	
Проверявайте заглавните части на IP пакетите	
Приложете необходимите правила	
Контролен списък за проверка на мрежите	
Използвайте криптирани съобщения по отношение на сериозни бизнес трансакции	
Записвайте и обработвайте данните за мрежовия трафик	
Засичайте познати атаки	
Засичайте аномалии	
Засичайте злонамерен трафик на данни	

О. Терминологичен речник

Актив: като актив възприемаме цялата информация, всички данни, устройства, компютърни системи, съоръжения и услуги, които осигуряват информационните дейности. Поради това в това определение можем да включим и хората, чиято работа е свързана с информационните компютърни системи. В контекста на въпроса за Киберсигурността, всички активи следва да бъдат защитени.

Заплаха: Всяко възможно нарушение, което може да предизвика пробив в сигурността и вреда на актив. Това нарушение може да бъде нарочно (преднамерено), случайно или дори вследствие на природно бедствие.

Агент-заплаха: Всяко лице или единица, което иска да причини вреда на актив преднамерено или причинява такава по случайност, например някой изключва сървъра по грешка или физически се удря в система.

Уязвимост: недостатък или слабост в дизайна или приложението на актив, които могат да създадат риск за актива или да се използват от агент-заплаха, за да се преодолее системата за сигурност. Примерите могат да варират от най-високорискови проблеми като некачествени резервни копия до недотам сериозни като просто лошо написан код.

Exploit: всеки софтуер или инструмент, който преднамерено се използва за постигане на преимущество над или уязвимост на актив, която да причини неизправност или анормална функционалност по един или друг начин. Очевиден пример са инструментите за хакване.

Защитна стена: При оперирането с компютърни системи, защитната стена се възприема като система за мрежова сигурност, която следи и контролира входящия и изходящия трафик в мрежата въз основа на предварително определени правила за сигурност. Защитната стена в общи линии създава бариера между една сигурна вътрешна мрежа и друга несигурна външна мрежа, каквато е например Интернет.

Риск: това е вероятността една потенциална заплаха да се възползва от определена уязвимост на актив и по този начин да нанесе вреди. Тъй както във всички теории, които почиват на вероятности, тук рискът може да бъде по-голям

или по-малък в зависимост от влиянието на различни фактори. Например можем с убеденост да твърдим, че съществува по-голям риск от загуба на данни, ако имаме само едно резервно копие на информацията, както и че рискът от атака срещу банков сървър е по-голям от риска от атака срещу сървър за съхранение на снимки.

Атака: това е всяко преднамерено действие, което уврежда или цели да увреди актив, независимо дали чрез простото му получаване (пасивна атака) или чрез променянето, унищожаването или изтриването му, включително и чрез разкриването му, без изрично оторизирано позволение за това (активна атака). Като примери могат да бъдат посочени атаките за отказ (блокиране) на услуга, пробиви в сигурността и други.

Повреда: под повреда се разбира всяко случайно събитие, което уврежда актив, например чрез физическото унищожаване на оборудване.

Намаляване на риска: това е всеки инструмент, услуга или система, която намалява риска от атака.

Компенсаторен контрол: под компенсаторен контрол се разбира всеки инструмент, услуга или система, които намаляват риска от атака срещу актив, като целенасочено попречат (застанат на пътя) на заплахата. Такъв пример е функцията на защитната стена в обмяната на между компютърна система и Интернет.

Свързано лице: това е лице, до което се отнася и който е свързан с определена информация.

Терминологичният речник е създаден въз основа на определенията дадени в източници: [5] [12], [13], [14], [15], [16], [20].

Р. Заключения (Изводи)

Поддържането на сигурността на една система, която с свързана с мрежата, се явява сложен проблем, но справянето със същия може да се улесни чрез прилагането на някои специфични предварителни предпазни мерки, чрез следването и спазването на определени сертифицирани процедури и протоколи, както и чрез придържане към доказани разрешения при възникването на проблем.

Важно е да отбележим, че всички системи трябва да са в съответствие с триадата основни принципи на ЦРУ относно информационната сигурност по всяко време, а именно: Конфиденциалност, Цялостност и Годност. Иначе казано, ако не покривате изискванията на триадата принципи на ЦРУ по отношение на всяка система и процес във вашия бизнес, то най-вероятно ще имате проблеми със сигурността по едно или друго време. За да избегнете това и да минимизирате възможността за настъпване на бъдещи проблеми и рискове, вие трябва да вземате предвид тези принципи на всеки етап от жизнения цикъл на системата, като следва и редовно да правите оценка на сигурността си, което ще спомогне за генералното ѝ подобряване.

Q. Източници

[1] Gasser, Morrie (1988). Building a Secure Computer System (PDF). Van Nostrand Reinhold. p. 3. ISBN 0-442- 23022-2,

[2] TechTerms - https://techterms.com/definition/vpn

[3] Denial-of-Service Attack - https://en.wikipedia.org/wiki/Denial-of-service_attack

[4]https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

[5] Introduction to Cybersecurity for Business, University of Colorado System on Coursera, Taught by: Greg Williams, Lecturer Department of Computer Science

[6] CS682: Advanced Security Topics Course by Dr. Elias Athanasopoulos, University of Cyprus (2018, https://www.cs.ucy.ac.cy/courses/EPL682/)

[7] V-Alert Project, LLP Funded

[8] https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

[9] https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/

[10] https://www.microsoft.com/en-us/download/details.aspx?id=12273

[11] https://haveibeenpwned.com

[12] https://en.wikipedia.org/wiki/Asset_(computer_security)

[13] https://en.wikipedia.org/wiki/Threat_(computer)

[14] https://en.wikipedia.org/wiki/Vulnerability_(computing)

[15] https://en.wikipedia.org/wiki/Exploit_(computer_security)

[16] https://www.techopedia.com/definition/6060/attack

[17] https://www.avg.com/en/signal/what-is-malware

[18] https://www.veracode.com/security/computer-worm

[19] https://www.eugdpr.org/

[20] https://www.techopedia.com/definition/1793/cyclic-redundancy-check-crc

[21] Furnell, S.M., Jusoh, A. & Katsabas D. (2006). The challenges of understanding and using security: A survey of end-users. Computers & Security, Vol.25: 27–35. Retrieved 10 March 2009 from http://linkinghub.elsevier.com/retrieve/pii/S0167404805002038

[22] Whitten, A. & Tygar, J.D. (2005). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: Cranor, L. & Garfinkel, S. (Eds.), Security and usability: Designing secure systems that people can use. Sebastopol, CA: O'Reilly, pp 669–692.

[23] Flenchais, I. & Sasse, M.A. (2007). Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. International Journal of Human Computer Studies. DOI:10.1016/j.ijhcs.2007.10.002

[24] https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html

[25] https://www.nist.gov/cyberframework

[26] https://www.iso.org/isoiec-27001-information-security.html

[27] https://www.cisecurity.org/

[28] http://www.alphr.com/realworld/380632/how-to-deal-with-a-ransomware-attack

[29] http://www.thewindowsclub.com/what-to-do-after-ransomware-attack

[30] https://www.quora.com/How-do-I-use-my-computer-after-a-Ransomware-attack

[31] https://www.tomsguide.com/us/ransomware-what-to-do-next,news-25107.html

[32] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 31-35

[33] https://en.wikipedia.org/wiki/Drive-by_download, access 27.01.2018

[34] https://en.wikipedia.org/wiki/Watering_hole_attack, access 27.01.2018

[35] https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf, access 27.01.2018

[36] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 36-39

[37] https://en.wikipedia.org/wiki/SQL_injection, access 27.01.2018

[38] https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/, access 27.01.2018

[39] https://www.acunetix.com/websitesecurity/cross-site-scripting/, access 27.01.2018

[40] https://blog.udemy.com/php-injection/, access 27.01.2018

[41] https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos, access 27.01.2018

[42] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 45-48

[43] Zulfikar Ramzan, Phishing attacks and countermeasures, Mark Stamp, Peter Stavroulakis, Handbook of Information and Communication Security, Springer, https://books.google.com/books?id=I-9P1EkTkigC&pg=PA433, p. 433-447

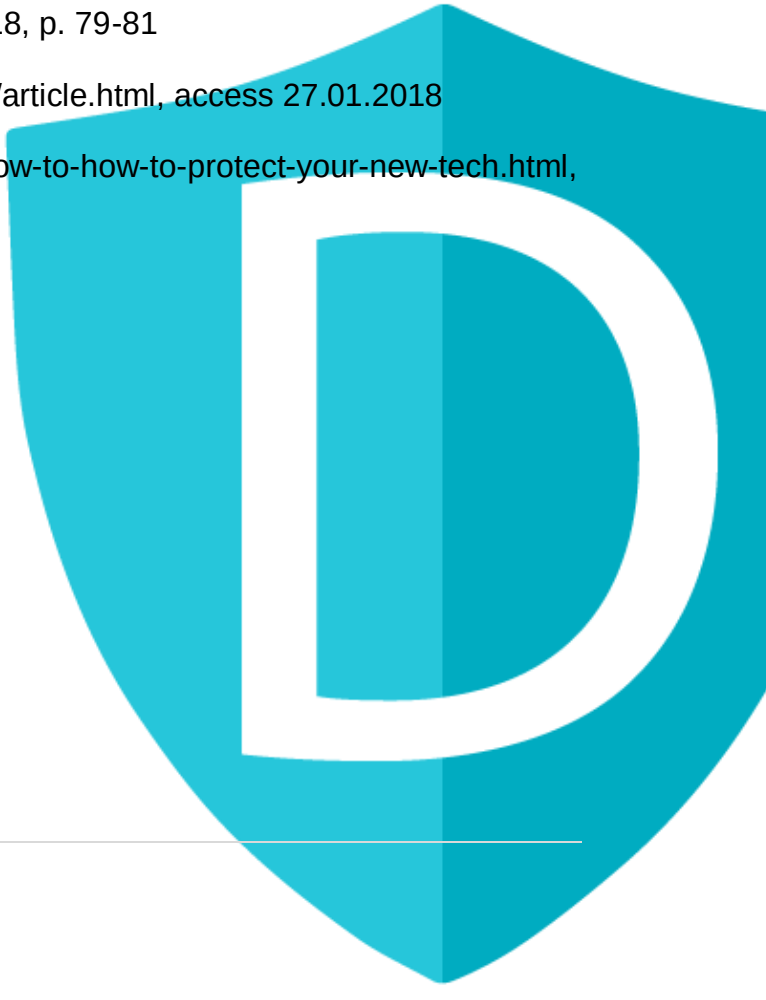
[44] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 64-67

[45] https://www.lifelock.com/education/how-common-is-identity-theft/, access 27.01.2018

[46] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 79-81

[47] https://www.pcworld.com/article/141474/article.html, access 27.01.2018

[48] https://us.norton.com/internetsecurity-how-to-how-to-protect-your-new-tech.html, access 27.01.2018



ЧАСТ V

ОЦЕНКА НА РИСКОВЕТЕ ЗА ДИГИТАЛНАТА СИГУРНОСТ

Списък с абревиатури

Abbreviation	Definition
DDoS	Distributed Denial of Service
DoS	Denial of service
ICT	Information and Communication Technologies
LFI	Local File Inclusion
PHPi	PHP injection or PHP Object Injection
RFI	Remote File inclusion
SQLi	SQL Injection attacks
XSS	Cross-site Scripting

A. Въведение

През последните години се забелязва чувствително повишаване на заплахите за дигиталната сигурност, както и на инцидентите, свързани с нея. Тези най-разнообразни по вид заплахи и инциденти причиняват сериозни последици, както икономически, така и социални, както за публичния сектор (държавните учреждения), така и за частните организации, и това е без дори да споменаваме засягането на отделните лица. Могат да бъдат дадени различни примери за последиците, които горепосочените причиняват, а именно: финансови загуби, загуба на клиенти и/или доверие от партньорите, уронване на репутацията на организациите, разстройване на организационните операции и други. В наши дни икономическите дейности са тясно свързани с обработката на данни и разчитат на последните за правилното си функциониране. Информационните и Комуникационните Технологии (ИКТ), както и разбира се Интернет, вече са от изключително значение за правилното функциониране на икономиката. Правителства, обществени и частни организации, отделните хора – днес всички сме зависими, по един или друг начин, от дигиталните технологии. Такива явления като “Big Data” и “Internet of Things” осигуряват голям потенциал за прилагането на иновативни методи по отношение на различни продукти и услуги, но те също така оказват влияние върху разбирането за мащаба и обхвата на дигиталната сигурност. Няма нужда да споменаваме броя на сайтовете, които биват хакнати всеки ден или пък броя на вирусите, които се създават всеки месец. Поради това, разработването на стратегии за осигуряване на дигиталната сигурност се явява не само нужно, но и жизненоважно за нормалното протичане на икономическите и социалните дейности. В този смисъл прилагането на процедури за оценка на риска може да ви помогне да обезпечите дигиталната си сигурност, както по отношение на икономическите си дейности, така и по отношение на социалните такива.

Оценката на риска е процес по установяване, анализиране и преценяване на потенциални опасности, пред които може да бъде изправена една организация и които могат да окажат влияние върху нормалното извършване на дейността на последната. Оценката на риска също така има за цел да осигури конкретни мерки

и механизми за намаляването на възможните опасности при извършването на настоящи и бъдещи бизнес операции [1]. За да може да се извърши оценка на риска, организацията трябва на първо място да установи възможните рискове и да определи вероятността от настъпването на такива заплахи. Оценката на риска е от полза при: планиране на проекти, подобряване на безопасността на работното място, организиране на събития, планиране на промени в работната среда (нови конкуренти, промени в правителствените политики) и други [2].

Дигиталната икономика дава възможност на организациите да разширяват дейността си все по-бързо, но това скоростно напредване на технологиите, оказва се, едновременно поставя и предизвикателства във връзка със сигурността пред тях. Следва да отбележим, че рисковете за дигиталната сигурност представляват грижа не само за малките предприятия, но и за големите организации. Следователно, оценката на риска е единственият начин, за да сте сигурни, че избраните от вас мерки за киберсигурност наистина съответстват на рисковете, пред които може да се изправи организацията ви. При оценката на риска една организация преценява вероятността за настъпване на определен риск, както и евентуалните последици от настъпването на последния [3], Оценката на рисковете в дигиталната сигурност има за цел да гарантира, че времето усилията и ресурсите ви не са пропилени в прилагането на механизми за защита срещу опасности, които едва ли ще се случат наистина, или дори да се случат, те няма да окажат сериозно влияние върху организацията [4].

Цифровата екосистема в наши дни е от особено голямо значение за икономиката и предвид наличието на нарастващите инциденти с дигитален характер от ОИСР подчертават, че изпълнителните директори и управителните органи на организациите трябва да третират дигиталната сигурност като икономически риск: “Рискът за дигиталната сигурност следва да се третира по-скоро като икономически, отколкото като технически проблем (…)” [5]. Това означава, че за организациите е важно да се интегрират механизми за оценка на рисковете за дигиталната сигурност, които след това да се вземат предвид при управлението на риска и процеса по вземане на решения.

Основната задача на тази глава е да предостави един цялостен преглед върху механизмите за оценка на рисковете за дигиталната сигурност, към които следва да се придържат потенциалните млади предприемачи в техните дигитални бизнес начинания, както и да подчертае важността от прилагането на тези стратегии за оценка на риска в областта на онлайн търговията.

Настоящата глава цели да предостави на потенциални млади предприемачи практически знания по отношение на техническите аспекти (Дигиталната Сигурност като технически риск), както и по отношение на икономическите аспекти (Дигиталната Сигурност като икономически риск) в сферата на Дигиталната Сигурност. Тя следва да осигури един цялостен поглед върху предимствата и недостатъците, които се проявяват при прилагането и/или при отказа от прилагане на механизма за Оценка на Риска в Дигиталната Сигурност.

Нещо повече, в съдържанието на главата са включени също практически съвети, както и примери за добри практики затова как Оценката на Риска в Дигиталната Сигурност трябва да бъде планирана и извършена в съответствие с установените принципни положения. В главата са включени и примери за стратегията, чрез която се прилага в действие механизмът за оценка на риска, а също така въпроси по отношение на организационното ѝ изпълнение в контекста на процесите по управление на риска и вземане на управленски решения. Друго полезно нещо е, че в главата са очертани възможните недостатъци и празнини при прилагането на механизма за оценка на риска, както и начините за справянето с тях.

На последно място, в настоящата глава се съдържа и изчерпателен терминологичен речник, както и контролен списък за Оценка на Риска за Дигиталната Сигурност, тъй като последните са необходими за цялостното разбиране на материята по посочения проблем.

B. Дигиталната сигурност като технически риск

Като вземем предвид нарастващото значение на Оценката на Рисковете за Дигиталната Сигурност и нуждата от прилагането на такава като част от процесите по управление на риска и вземането на управленски решения в различните организации, в тази глава ще се фокусираме върху техническите аспекти, тъй като механизмът за оценка на риска за дигиталната сигурност има както икономическа, така и техническа страна. В настоящата глава са описани отделните технически рискове във връзка с дигиталната сигурност, като са изведени подходящи мерки за справяне с вече установени рискове. Съдържанието ѝ е построено въз основа на сравнителна съпоставка на предимствата и недостатъците, които се открояват вследствие на прилагането/неприлагането на стратегиите за оценка на риска .

Съществуват много различни дигитални рискове за бизнеса и организациите, които могат да се породят в отделни отрасли и сектори, които са с различни размери на предприятията и притежават различна степен на сигурност. Поради това е важно всички правителства, всички публични и частни организации, както и отделните физически лица да се научат да управляват и намалят рисковете за дигиталната си сигурност. Дигиталната сигурност като технически риск представлява и тема от особено значение за потенциалните млади предприемачи, които следва да са запознати с нея при започване на своите бизнес начинания. Това е така, тъй като този технически риск представлява директна заплаха за бизнеса, която може да доведе до загуба на загуба на финансови активи и уронване на авторитета на съответната организация.

В настоящата глава се разглеждат различните технически рискове по отношение на Дигиталната Сигурност, като например: малуер, уеб-базирани атаки, атаки чрез уеб приложения, фишинг, спам, отказ от услуги, софтуер за изнудване, ботнети, вътрешни заплахи, физическо манипулиране, пробив в сигурността, кражба на самоличност, изтичане на информация, exploit kits, кибер-шпионаж, както и други рискове, които са описани детайлно в тази глава, наречена „Киберсигурност“.

Гореизброеният списък с различните технически рискове най-общо представлява сбора от техническите заплахи през 2017г., които са посочени в Доклада относно заплахите за сигурността за 2017 на Агенцията за мрежова и информационна сигурност към Европейския съюз (ENISA) [6].

Като знаем определението за **Малуер**, посочено в глава “Киберсигурност” и най-разпространените видове малуер като: вируси (които заразяват програмни и/или лични файлове), червеи (които могат да правят свои копия през мрежата), шпионски софтуер и кийлогъри (които събират личната информация на потребителя), Троянски коне (които изглежда и могат дори да функционират като легитимен софтуер, руткит (който получава администраторски права в операционната система с намерението да уврежда), browser hijackers (които променят настройките на вашия уеб браузър), malvertising (използването на надеждни системи за онлайн реклама с цел разпространяването на злонамерен софтуер), нека сега да определим различните технически рискове във връзка с този аспект от Дигиталната Сигурност [7].

Когато горепосочените заплахи са на определено устройство или се предадат по мрежата, те могат да използват (източат) ресурсите на вашето устройство или мрежа и по този начин да забавят Интернет връзката ви. Съществуват и други технически рискове, произтичащи от тези заплахи, като малуерът може да:

- унищожи или повреди вашите лични или бизнес файлове,
- деактивира антивирусната програма или дори да затрудни функционирането на вашия уеб браузър, с цел да предотврати изтеглянето на инструменти (програми), с които да се премахнат вирусите,
- запаметява клавишни комбинации, чрез които да откраднат номерата на кредитните ви карти и паролите ви,
- получи достъп до вашия уеб браузър или устройство, за да: го използва за търговски цели или злонамерено, като ви пренасочи в уебсайт, който да се опита да ви заблуди да въведете паролите на акаунтите си ,
- изпраща свои копия на вашите имейл контакти [8].

По-долу може да намерите селекция на най-важните и подходящи мерки за предотвратяване на заплахи и справянето с установени рискове, които са породени от малуер:

- използвайте само лицензирани копия на софтуер и/или теглете софтуер само от познати и надеждни източници;
- инсталирайте само софтуер, които е необходим за устройството ви, тъй като допълнителният софтуер, който не се използва, представлява допълнителна заплаха,
- съхранявайте оригинални копия на софтуера си на безопасно място (локация),
- правете копия на файловете и системата си често и ги съхранявайте на безопасно място,
- обновявайте редовно вашите: операционна система, уеб браузър, антивирусните ви системи, антишпионски софтуер, както и всички инсталирани програми,
- не използвайте софтуер, дискове, преносими дискове и други устройства и системи, които използвате в дома си.

Уеб-базираните атаки, които се възползват от уеб-активиращите се системи и услуги, също са описани в глава “Киберсигурност”. След прочитането на тази глава вие вече сте запознати с различните видове такива атаки, а именно: web browser exploits (злонамерен код, който използва уязвимостите в операционната система или в инсталиран софтуер), web servers and web services exploits (които се възползват от грешка или уязвимост на уеб сървър или уеб услуги), drive-by attacks (нежелано изтегляне на компютърен софтуер от Интернет), water-holing attacks (заразяване на избрани уебсайтове с малуер), man-in-the-browser-attacks (прихващане на чувствителна информация и данни). След това изброяване, вече можем да пристъпим към описване на различните технически рискове, които се пораждат във връзка с Дигиталната Сигурност:

- web browser exploits могат да ви заблудят чрез адресната лента на браузъра, в който случай потребителят вижда привидно надеждно URL (например за онлайн банкиране) в лентата, но съдържанието на уебсайта се контролира от

атакуващия. Този метод може да се използва за кражба на информация за достъп до различни системи от данни [9],

- web servers and web services exploits могат например да използват уязвимост като Cross Site Scripting, при която атакуващият може да инжектира злонамерен код в иначе надежден уебсайт или приложение. Тези способи могат да се използват за събиране на данни от уеб страницата, получаване на достъп до потребителските сесии, пренасочване на потребители и събиране на информация относно преглежданото съдържание от потребителя [10],
- drive-by атаките могат да инсталират кийлогъри, софтуер за изнудване на устройството или дори да създадат задна врата, която позволява на атакуващия да инсталира дори повече малуери. Този вид атаки могат да се използват за криптиране на данни на определено устройство с цел искане на откуп, както и за събиране на пароли, информация за профили и чувствителна информация, за да се получи неоторизиран достъп или за извършване на неоторизирани транзакции [11],
- water-holing атаките се използват, за да се атакуват предварително определена група потребители, използвайки злонамерен код, с намерение да се откраднат данни или да се поеме контрол над системите в организация, индустрия или цял регион. Тези атаки могат да доведат до заплахи за множество организации, включително здравни, технологични, образователни, правителствени и други.[12]
- man-in-the-browser атаките често са използвани за кражба на еднократни пароли (SMS), които банките използват за удостоверяване на парични преводи на потребители. В тези случаи, когато устройството е заразено с man-in-the-browser троянски кон и потребителят посети сайта за онлайн банкиране, тази сесия задейства вируса, който може да промени номера на сметката и/или сумата по банковия превод като в същото време на потребителя се показва уебсайта с първоначалните данни за транзакцията [13].

С оглед горепосоченото можем да кажем, че уеб-базираните атаки са често използвани за: кражба на потребителски данни, пароли и друга информация за

достъп/еднократни пароли, с цел да се получи неоторизиран достъп до системи или извършване на неоторизирани транзакции, извършени посредством онлайн банкиране. Тези атаки представляват сериозна заплаха както за отделните потребители, така и за различните организации, поради което е от особена важност да се вземат подходящи мерки с цел предотвратяването и управлението на установени рискове. Ето някои стъпки, които може да предприемете, за да предотвратите настъпването на такива рискове:

- инсталирайте антивирусен и антишпионски софтуер, като ги обновявайте редовно,
- винаги дръжте операционната си система и уеб браузъра си обновени,
- конфигурирайте мерките за сигурност на вашия уеб браузър (например: използвайте блокиране на изскачащи прозорци, не запазвайте паролите си),
- използвайте Internet като сте регистрирани на вашия компютър като потребител, който няма административни правомощия,
- преглеждайте вашите имейли във вид на обикновен текст, а не във HTML изглед,
- използвайте предплатена кредитна карта, когато правите покупки от Интернет,
- не използвайте вашето онлайн банкиране през ненадеждни устройства или мрежи,
- пишете адреса на уебсайта ръчно и не вярвайте винаги на лентата на състоянието [14].

Също така, популярността на такива ресурси, както и на проекти, базирани на отворен или публичен код като приставките Joomla и Wordpress, сайтовете Magento и др., имат значение по отношение на Дигиталната Сигурност. Както може би вече знаете от глава „Киберсигурност“, **атаките чрез уеб приложения** засягат приложно-програмния интерфейс (API) на уеб приложенията. В горепосочената глава може да прочетете повече относно тези видове атаки: SQL инжектиране (SQLi – техника за инжектиране на код), Local/Remote File Inclusion (LFI/RFI – уеб приложение включва файлове на уеб сървър), Cross-site Scripting (XSS – прилагане на зловреден скрипт в надежден сайт), PHP инжектиране или

PHP обектно инжектиране (PHPi – извършване на различни видове злонамерени атаки).

Уеб приложенията в модерния свят вече не са ограничени само до представянето на текст и картинки, подобно на хартиена брошура. Рисковете за сигурността на такива приложения може да представляват пряка заплаха за организации, тъй като в наши дни всички лични и бизнес потребители използват приложения ежедневно. В този смисъл уеб приложенията се оказват ключови инструменти, които позволяват на частни потребители, организации, клиенти и дори държави да поддържат комуникация, да имат достъп до информация и да обработват последната. Тази информация може да включва например: финансова информация, медицински досиета, данни във връзка с националната сигурност и други. [15].

Ето някои примери за технически рискове по отношение на Дигиталната Сигурност:

- пробив в механизмите за защита на системите,
- получаване на информация, която не би трябвало да е достъпна извън приложението и/или организацията (например интелектуална собственост),
- получаване на неоторизиран достъп до уеб приложения и съхраняваните в тях данни (например: имена, номера на кредитни карти и всякакъв друг вид конфиденциална и чувствителна търговска информация),
- шпиониране на браузъра (манипулирането на бисквитки може да позволи на неоторизиран потребител да се представи за оторизиран такъв),
- повишаване на възможностите на оторизиран потребител,
- кражба на самоличност, кражба на устройство или съдържание, както и измами с кредитни карти,
- отказ на услуга.

Тъй като уеб приложенията се развиват и с това поддържането на тяхната сигурност придобива все по-голямо значение, ние следва да посочим най-важните и подходящи мерки за предотвратяване на установените заплахи:

- програмата за управление на риска е от особено значение, чрез изработването на политики и процедури следва да се спре внедряването на уеб приложения, които са уязвими,
- използване на програмисти, които провеждат обучения относно добри практики в кодирането,
- уеб приложенията трябва да се тестват от професионалисти, които да проверят нивото на тяхната сигурност, преди да бъдат пуснати в експлоатация [16],
- обновяване на пачовете за сигурност на уеб сървъри и уеб приложения,
- използване на Система за Засичане на Нарушения (IDS) и Система за Предотвратяване на Нарушения (IPS),
- използване на актуални защитни стени (при които има възможност да се отхвърлят злонамерени пакети),
- сканиране за уязвимости на кода със специализиран софтуер, след като приложението е вече разработено,
- използване на софтуер за сканиране на уеб сървъри, който търси потенциални опасни файлове на сървърите. [15].

Също така, следва да се посочат следните възможни проблеми:

- „осиротели“ уеб приложения (разработени от екипи, които вече не работят за компанията или такива приложения, които вече не се поддържат),
- „наследствени“ уеб приложения (стари уеб приложения, разработени преди внедряването на политики за сигурност),
- кратък период до пускане на пазара на уеб,
- изработени по поръчка уеб приложения (разработките на вътрешни приложения са с висок риск от човешка грешка),
- повишаване на рисковете за сигурността на уеб приложения [17].

Поради факта, че **фишингът** е особено популярна Интернет измама, важно е да включим и него в Оценката на Рисковете за Дигиталната Сигурност.

Успешното извършване на фишинг атака може да доведе до технически рискове, като например:

- използване на вашия компютър за инсталиране на вируси и червеи,

- изпращане на фишинг имейли до всичките ви контакти в имейла,
- използване на крадени данни с цел получаване на достъп до системата на организацията и нарушаване на механизмите за системна сигурност,
- използване на крадени лични данни за откриване на фалшиви банкови сметки или кредитни карти, които впоследствие да бъдат използвани за незаконни транзакции,
- използване на акаунта ви за вашето онлайн банкиране с цел извършване на измамни банкови преводи или правене на онлайн покупки.

Горепосочените технически рискове могат да доведат и до такива икономически рискове, като финансови загуби, уронване на репутацията.

За намаляването на тези рискове следва да се въведат следните мерки:

- установяване на отделите, които е най-вероятно да бъдат засегнати от фишинг,
- разработване на защита от фишинг и план за действие при такава атака,
- обсъждане на плана както със служители във вашата организация, така и с външни за организацията страни (партньори, клиенти и други),
- обучение на служителите [18].

Спамът може да бъде изпратен от ботнети или от заразени с вируси компютри, но той представлява проблем и в социалните мрежи, каквито са: Facebook, Twitter и LinkedIn. С помощта на спам атаки в социалните медии, измамниците могат да получат достъп до профилните страници на потребителите, на които после да публикуват линкове, картинки и видеа. Спамът е проблем, който обхваща и мигновените съобщения в социалните мрежи, като се забелязва, че спамерите се насочват от имейлите към социалните мрежи. Добре, но какви са техническите рискове, породени от спам:

- заразяване на компютри, уеб приложения, сървъри и мрежи с вируси и/или със зловреден код,
- спам имейлите заемат място в сървърите на електронната поща,
- спам имейлите могат да генерират голям брой сървърни заявки и дори могат да причинят срив на работата на сървъра, като оставят съответната организация без електронна поща,

- устройства, които са заразени чрез използване на спам, могат да станат част от ботнет, да стартират малуер, да изпращат спам съобщения или да вземат участие в Разпределени Атаки за Отказ на Услуга (DDoS).

Организациите могат да се защитят от спам и от други негативни последици, които произтичат от спама, чрез:

- използване на антиспам инструмент на вашия имейл сървър и обновяване на последния редовно; антиспам инструмента следва да сканира всички входящи и изходящи имейли за спам и малуер,
- антиспам инструментът следва да използва техники като например: филтриране на достъпа до уебсайтове или на съвпадащи модели, като целта е засичането на нови спам кампании,
- настройване на аларми, които да известяват в случай, че имейл сървърът на организацията ви е станал част от ботнет; целта е да се осигури използването на инфраструктурата на организацията по законен начин [19],
- също така, потребителите трябва да се образоват: да не изпращат отговор на спам имейли; да не кликват на каквито и да е линкове за инсталиране/отваряне на файлове в спам имейли; да не препращат имейли от непознати, да използват спам филтър и да докладват спамове [20],
- в социалните медии вие трябва: да не използвате приложения, в чиято надеждност не сте сигурни; пазете се от подозрителни линкове, които са публикувани в социална мрежа или са изпратени чрез мигновено съобщение,
- винаги изтривайте от профилите си в социалните мрежи приложения, които не са ви познати,
- изтривайте всички публикации/съобщения, които са публикувани/изпратени от ваше име чрез приложения, като същевременно уведомете вашия контакт, че е възможно да сте им изпратили спам съобщение [21].

Вследствие на това, че повечето организации използват уеб приложения и сървърни инфраструктури за техните ежедневни операции, защитата на уеб приложенията и сървърите от **Атаки за Отказ на Услуга (DoS) и Разпределени Атаки за Отказ на Услуга (DDoS)** е нещо, за което организациите несъмнено трябва да се погрижат. DoS или DDoS атаките предизвикват невъзможност за достъп до сървъра на служители, членове или акционери в организацията, т.е.

услугата не може да се предостави на легитимираните ѝ потребители. Нещо повече, този вид атаки крият и други технически рискове, а именно:

- висока консумация на широчина на честотната лента или на изчислителната мощ на компютрите,
- те принуждават IT служителите да се фокусират върху разрешаването на този проблем, като през това време атакуващият може да осъществи друга атака и да се фокусира например върху кражба на данни,

В тези случаи е възможно и настъпването на нетехнически рискове, които са свързани със загуба на приходи и уронване на авторитета на съответната организация [22].

Какъв следва да е отговорът на Атака за Отказ на Услуга и Разпределена Атака за Отказ на Услуга и как да намалим риска от извършване на такива атаки:

- отблъскване на атаката с помощта на защитна стена – това е най-лесният вариант,
- евентуално да се ограничи: входящият трафик от определени IP региони, броят на кошниците, които потребителите могат да създават, броят на запитванията към функцията за търсене на уебсайта,
- увеличаване на ефективността на уебсайтовете, уеб приложенията и системите чрез повишаване на обработващите мощности,
- окуражаване на добрите практики в кодирането (например чрез ограничаване на възможностите за претоварване на търсачката на уебсайта),
- използване на инструменти за мониторинг с цел анализиране на входящия трафик и установяване на злонамерени заявки,
- разберете предварително какви мерки могат да предприемат вашият Интернет доставчик или уеб хостинг компания при наличието на DoS/DDoS атаки [23].

В глава “Киберсигурност”, както и досега в настоящата глава, ние вече няколко пъти използвахме думата **ботнет**. Но какви са техническите рискове, които произтичат от тази заплаха? Когато едно устройство е заразено:

- източва се мощността на компютъра или мрежата, за да улесни изпълнението на задачите на нападателя; boots drain the device computing
- това води до висока консумация на честотна лента,
- и кражба на чувствителни данни,

Налице са и нетехнически рискове във връзка с атаките, които могат да се изразят във високи разходи за Интернет трафика и увреждане на авторитета на организациите, когато е засегната инфраструктурата вследствие на атаките.

Организациите могат да предприемат различни мерки с цел да предотвратят рисковете от ботнет атаки:

- мониторинг на ефективността на мрежата и мрежовия трафик, за да се засича необичайно поведение в мрежата,
- всички мрежи, сървъри и устройства трябва да бъдат обновявани редовно,
- използване на анти-ботнет инструменти (защитни стени, антивирусен софтуер, пакети за откриване на руткит и специализирани антибот програми) с цел намиране и блокиране на бот вируси,
- бързо премахване на бот вируси и елиминиране на уязвимостите в сигурността,
- също така, потребителите трябва да са образовани: не трябва да кликват върху всякакви линкове или файлове за изтегляне/отваряне на спам имейли [24].

Друга заплаха в пейзажа на Киберсигурността представляват **вътрешните заплахи**, които бяха разгледани в глава “Киберсигурност”. Защо тези заплахи са толкова важни? Съществуват много причини, но сме длъжни да посочим поне по-значимите, а именно:

- засичането на преднамерени действия е трудно, тъй като е трудно те да се разграничат от безопасната дейност – нормалната работа на служители,
- обикновено злонамерените служители знаят как да прикрият действията си, затруднявайки доказването на тяхната вина (най-често ще се опитат да обяснят, че е станала грешка).

Как можем да разпознаем такива злонамерени служители? Това са:

- служители, които изтеглят данни на външни дискове,
- служители, които преглеждат данни, които не са свързани с тяхната работа,
- служители, които изпращат по имейл данни до своите лични имейл профили,
- служители, които заявяват по-високо ниво на достъп, без да имат нужда от такова,
- служители, които често излизат извън офиса в работно време,
- служители, които нарушават политиките на организацията,
- служители, които твърде много използват принтери и скенери,
- служители, които инсталират софтуер, който не им е нужен за тяхната работа,
- служители, които се опитват да получат достъп до зони с ограничен достъп [25].

Нарушението на сигурността и **кражбата на самоличност** като специален случай на такова нарушение, водят до сериозни последици и са тясно свързани с много от гореизброените проблеми във връзка с рисковете за Дигиталната Сигурност. Самите две нарушения бяха разгледани в глава „Киберсигурност“, като в тази глава само ще изброим списък с определени подходящи мерки, които следва да помогнат за предотвратяването на тези рискове:

- разработете и въведете план за действие при загуба на данни,
- образовайте служителите си във връзка с обработката и защитата на данни, като им предоставите и техническа помощ,
- не събирайте данни, които не са ви нужни,
- не съхранявайте данни на много различни места,
- поддържайте своите приложения и системи винаги обновени,
- запомнете, че криптирането на данни не следва да е единствения метод за вашата защита,
- изисквайте прилагането на същите стандарти от вашите доставчици и партньори [26].

Специално внимание е необходимо да се обърне и по отношение на намаляването на риска от това да станете жертва на кражба на самоличност. За да се предпазите, вие трябва:

- да намалите броя на кредитните и дебитни карти, които притежавате,

- да ограничите броя на финансовите институции, които ви обслужват,
- да използвате предплатени карти, когато пазарувате онлайн,
- никога да не давате номера на вашата кредитна или дебитна карта, както и останалата ви лична информация по телефона, чрез имейл или през незащитени уебсайтове,
- да се свържете с издателя на вашата кредитна или дебитна карта, когато очаквате последната да е преиздадена и да пристигне, но тя все още не е във вашата пощенска кутия,
- да правите ежегодна проверка на вашата кредитна активност [27].

За съжаление, вие не можете да предпазите себе си напълно, така че ако крадец иска да открадне личната ви информация, неговите или нейните шансове са изключително високи [28].

C. Дигиталната Сигурност като икономически риск

След като вече познаваме техническите аспекти на рисковете за Дигиталната сигурност, следва да се запознаем и с икономическите аспекти на този въпрос. Целта на настоящия раздел е да се разясни влиянието на Дигиталната Сигурност върху икономическите аспекти на предприемачеството, като следва да се обърне внимание не само на икономическите, но и на социалните дейности, които са нужни, за да се осигури едно по-високо ниво на Дигитална Сигурност по отношение на младите предприемачи и техните бизнес начинания.

Икономическото измерение на дигиталната сигурност би следвало да е от особен интерес за потенциалните млади предприемачи що се отнася до техните бизнес начинания, тъй като рисковете за дигиталната сигурност по-скоро трябва да се изследват като икономически, а не просто като технически въпрос. Това означава, че за тях е от голямо значение да се въведат механизми за оценка на рисковете за дигиталната сигурност, които механизми да станат неизменна част от цялостния процес по управление на риска и вземане на управленски решения в съответната организация. Всички заинтересовани страни, включително потенциалните и настоящите млади предприемачи, следва да са наясно, че рисковете за дигиталната сигурност могат да окажат влияние върху постигането на техните икономически и социални цели. За да са наясно с тези рискове, потенциалните и настоящи млади предприемачи трябва да притежават знанията и уменията, които са нужни за разбирането на риска и влиянието на управлението на рисковете за дигиталната сигурност върху техните предприемачески дейности. Тези лица също така трябва да знаят, че не е възможно да се предпазят от рисковете напълно, като заради това е нужно да се справят с определено ниво на рискове за дигиталната сигурност, ако искат да постигнат своите икономически и социални цели. Друго важно нещо е това, че процесът по управление на рисковете за дигиталната сигурност трябва да спазва интересите и на трети страни, и на обществото като цяло [29].

Дигиталната Сигурност може да бъде разгледана от поне четири различни перспективи, а именно: като технология, като правоприлагане, като национални и международни мерки за сигурност, както и като механизъм за икономическо и

социално благоденствие. Тъй като в настоящия раздел се разглежда дигиталната сигурност и нейното икономическо влияние, трябва да отбележим, че това влияние се изразява в аспекти като “материално благосъстояние, иновации, разрастване, конкурентоспособност и наемане на служители във всички икономически сектори, както и в някои други аспекти, като например: индивидуални свободи, здраве, образование, култура, демократично участие, наука, свободно време и други икономически измерения на благосъстоянието, чиито прогрес се благоприятства от дигиталната среда" [30]. И това е така, защото дигиталната среда е от особено значение за доброто функциониране на сегашните икономики и общества, като същевременно тя представлява и източник на иновации.

Инцидентите, свързани с дигиталната сигурност, могат да причинят различни по вид последици за засегнатите организации, като например уронване на репутацията (когато името на организацията е опозорено), загуба на конкурентоспособност (когато са откраднати търговски тайни), финансови загуби, които са пряка последица от атаката (например чрез усложнени измамни схеми), загуба на целия бизнес и прекратяване на търговските операции (например при саботаж), както и финансови разходи по възстановяване на бизнеса и/или съдебни дела и налагане на глоби. Налице е трудност да се оцени реалният размер на разходите при инциденти, които са свързани с дигиталната сигурност, тъй като организациите често предпочитат да не споделят тази информация, оценявайки последната като потенциално увреждаща техния бизнес. Поради това, към настоящия момент не съществуват статистики и данни изобщо, които да измерват истинските разходи, породени от такива инциденти. “Организациите, които са допуснали нарушение на дигиталната си сигурност, могат да претърпят неблагоприятни последици като налагане на глоби, поемане на разходи за обезщетение и други”. Друга икономическа последица от настъпването на подобен инцидент е смяната на служителите на ръководни постове в съответната организация. В миналото много изпълнителни директори и други ръководители са загубили работата си в резултат на нарушение на сигурността в организация, след като последното е било разкрито от медии. Важно е да се отбележи, че при самостоятелни търговци, както и при малки и

средни по размер предприятия, това нарушаване на сигурността може да доведе до значими икономически загуби, кражби на самоличност, а и до други неблагоприятни икономически последици. Отделните лица, разгледани като потребители, могат да загубят доверието си в целия сектор вследствие на нарушението, като това далеч надхвърля щетите [31].

С оглед гореизложеното е видно, че организациите и по-специално младите предприемачи следва да обезпечат благоприятното влияние на техните мерки за дигитална сигурност върху икономическите и социалните дейности на последните. Ясно е, че не може да бъде елиминиран всеки потенциален риск, но точно заради това трябва да бъдат взети определени решения, като се има предвид, че мерките за дигитална сигурност "могат да увеличат размера на финансовите разходи, сложността на използваната система и времето за търговия, както и да намалят производителността, използваемостта, възможността за развитие и иновации, а не на последно място и удобството на потребителите ви". Всички от горепосочените проблеми по естеството си представляват разходи. [32].

Управлението на рисковете за дигиталната сигурност изисква да се знае, че такива рискове в действителност съществуват, както и уменията за справяне с тях, които следва да се придобият (някои от тези умения могат да бъдат придобити и чрез настоящото електронно ръководство).

D. Интегриране на Дигиталната Сигурност като част от цялостния механизъм за управление на риска и процесът по вземане на управленски решения в организациите

След като вече познаваме различните технически и икономически рискове, то би следвало да виждаме ясно нуждата от интегриране на дигиталната сигурност като част цялостния механизъм за управление на риска и процеса по вземане на управленски решения в различните организации.

Звучи добре, но какво точно означава това? Нека да разгледаме следния пример: един клиент прави поръчка от нашия онлайн магазин половин час преди обяд, а в нашата политика за доставки е заявено, че ако клиент поръча нещо преди обяд, то последния трябва да получи поръчката си още на същия ден. Заради това се налага да бързаме да издадем и принтираме фактурата, за да можем да дадем пратката на куриера преди той/тя да тръгне със следобедните доставки и по този начин да успеем да доставим пратката навреме и да сме в съответствие с нашите политики. Това е една ежедневна и доста честа „извънредна“ ситуация. Тук съществува рискът от разпадане на Интернет връзката, което би ни попречило да издадем фактурата от нашия онлайн магазин. Налице е и риск от повреждане на отделните устройства (компютър или принтер), което пък ще ни попречи да принтираме фактурата. Това не е най-голямата криза за сигурността, както сами виждате, но дори тя, може да доведе до негодуването на клиенти, отказване на поръчки и евентуално до уронване на репутацията на организацията.

Добър начин за анализиране и разбиране на рисковете представлява разбиването им на следните области:

a) Местата, до които имаме достъп, могат да увеличат риска от компрометиране на нашата сигурност. Знаем ли дали уебсайтовете, в които влизаме са безопасни? Понякога, когато посетите даден уебсайт, вие можете да получите известие от вашия браузър, че съответния уебсайт не е сигурен. В

този случай имате възможност да напуснете сайта или да продължите, но какво трябва да направите?

А какво да кажем за софтуера? Знаем ли предварително дали софтуерът, който искаме да инсталираме е безопасен? Дори и той да е абсолютно безопасен, все пак съществува ли вероятност да са инсталирани твърде много приложения на устройствата ни, които да забавят тяхната работа? А възможно ли е да нямаме достъп до най-добрия софтуер за извършване на необходимите задачи, което да ни направи по-малко продуктивни? Свързваме ли нашите лични устройства с мрежата на организацията? Използваме ли не по предназначение компютърните устройства на компанията? Инсталираме ли или разглеждаме незаконни материали?

b) Обстоятелството към кои мрежи се свързваме може да повиши риска от компрометиране на принципите на цялостност и конфиденциалност по отношение на нашите системи. Можем ли да бъдем сигурни, че системата, към която се свързваме, е сигурна? Използването на мобилни устройства чрез несигурни мрежи, като например ползването на Wi-Fi мрежата на летище или свързването към мрежа на дадено кафене, може да се окаже застрашаващо и потенциално опасно за нашите устройства и за данните, които те съдържат.

c) Когато настъпят определени събития, рискът се повишава. Например, ако е налице някой природен катаклизъм и вие получите съобщение, в което се твърди, че е от Червения Кръст и в което те заявяват, че приемат дарения, ще повярвате ли веднага на това твърдение? В този случай трябва първо да проверим истинността на това твърдение.

d) Как следва да се придържаме към добрите практики относно сигурността? Спазваме ли най-добрите практики и имаме ли достатъчно познания по отношение на тях? Ако нямаме такива, тогава ще се наложи да направим проучване и научим повече за тях, преди да предприемем каквито и да било действия. И това е така, защото по-голямата компетентност означава поемане на по-малък риск.

e) Защо следва да прилагаме тези най-добри практики? Тук следва да можем логически да обосновем предприемането на отделните мерки във връзка с киберсигурността. Грешно е разбирането, че ще сме защитени, ако просто

следваме действията на тълпата или тези действия, които са посочени в някой определен уебсайт. Изследвайте, проучвайте, питайте, научете и разберете. Някои от мерките може да са добри за вашата компания, а прилагането на някои може да бъде и опасно. Познаването на естеството на действията ви също понижава рисковете за вашия бизнес. Така например, ако получите линк, на който трябва да кликнете или имейл, който трябва да прочетете, не го правете преди да разберете защо е нужно това. Друг пример в тази насока е ненужното използване на услуги за споделяне на файлове и данни, просто защото така е по-лесно, без да осъзнаваме заплахите, които могат да се породят от него. А какво би станало в случай, че забравите паролата си или пък забравите завинаги данните, с които удостоверявате самоличността си?

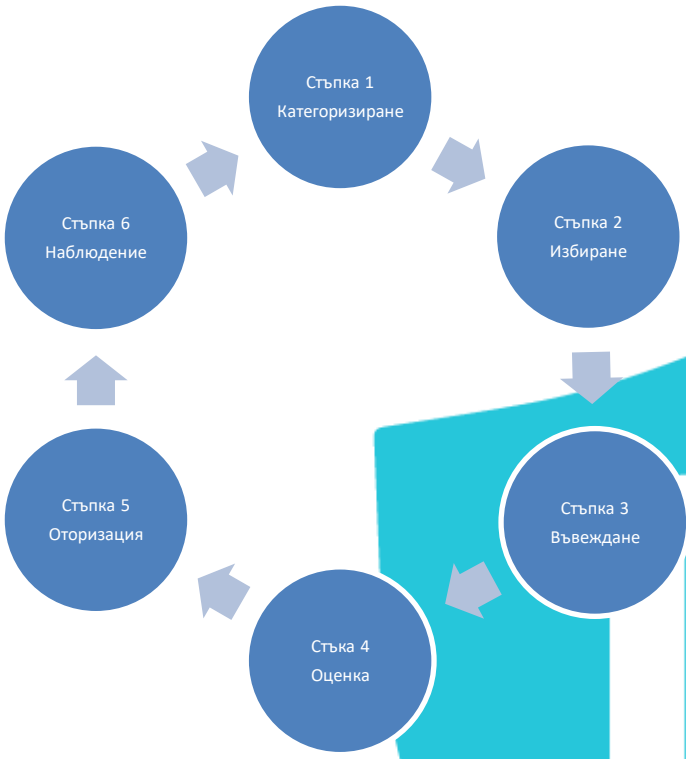
Нещо повече, за да разберете в цялост рисковете, трябва да вземете предвид и тези рискови фактори, които не сте в състояние да промените. Така например трябва да осъзнаете, че не можете да промените начина, по който действат операционните ви системи или софтуерът за продажби, макар и последните да имат някои уязвимости. Вие ще може да подобрите ефективността на тези системи само чрез въвеждането на определени мерки. Не трябва да забравяте също така, че ще има потребители, които ще отказват да спазват добрите практики, които прилагате по отношение на сигурността на вашия бизнес. В тези случаи вие ще трябва да се справяте с потребителите по различни начини, но без да компрометирате мерките за сигурност или киберсигурност на вашата организация.

За да може ефективно да управлявате вашия операционен и организационен риск, вие може да използвате **Рамка за Управление на Риска**; това е система от работни процеси, които целят да ви помогнат при управлението на риска. Но каква е разликата между операционен и организационен риск? Операционните услуги, системи или функции в рамките на организацията са свързани с операционния риск, докато цялостната структура на организацията се свързва с операционния риск. В рамката за управление на риска, сигурността и дейностите по управление на риска се разглеждат в тясна взаимовръзка по отношение на цялата система или целия жизнен цикъл на дейностите, което по същество

представлява изключително значителна стъпка към осигуряването на ефективна информационна система за сигурност.

Важна част за цялостната стратегия за вашия бизнес/организация следва да бъде Управлението на Риска. То ще ви помогне да си отговорите на въпроси като “Как да установим наличието на риск?” и “Как да се справим с този риск?”. NIST 800-37, която представлява рамка за управление на риска по отношение на жизнените цикли на системите в реално време, е добър пример за това.

Е, по какъв начин следва да приложите рамката за управление на риска? Жизненият цикъл на рамката за управление на риска предвижда редица стъпки, които могат да бъдат предприети с цел прилагането на собствена рамка за управление на риска (виж Фигура 1). Тези стъпки са очертани накратко в следващата фигура.



Фигура 1: Рамка за Управление на Риска [33]

Стъпка 1: Категоризирайте/определете самата система и как се използва тя. Важността на системата следва също да се вземе предвид, т.е. дали става въпрос за сървър със снимки или пък за система за кредитни карти.

В случай, че се касае за система за кредитни карти, това сървър за кредитни карти ли е или терминал? Ако тези сървъри бъдат „свалени“, как можем да ги оправим, така че отново да започнат работа? В тези случаи ще трябва да има ясно определени роли, така че да се знае кой е отговорен за предприемането на тези стъпки (т.е. собственика на системата).

Стъпка 2: Изберете мерките за сигурност, които ще приложите в системата си, като съобразите тяхното ниво на критичност (ниско, средно и високо). Както вече споменахме, не е добра практика прилагането на защитни мерки по отношение на всичко, тъй като това може да доведе до различни проблеми в представянето на системата - например в антивирусните изисквания следва да се определя дали от служителите се изисква специално заверяване, за да получат достъп до финансовите системи (в този случай е нужна). Тук, както и в предишната стъпка, отново трябва да определите кой ще бъде отговорен за изпълняването на тази стъпка (например служителят, който отговаря за сигурността на информацията).

Стъпка 3: Като следвате избора на мерки за сигурност в Стъпка 2, вие ще трябва да приложите тези мерки в настоящата стъпка (например да инсталирате съответния антивирусен софтуер на системите). Тук отново следва да назначите някой човек, който да е отговорен за изпълнението на тази стъпка (например собственикът на информационната система).

Стъпка 4: След като приложите на практика мерките за информационна сигурност, описани в предишната стъпка, в тази стъпка вие следва да разработите няколко процеса, чрез които да се уверите, че мерките за сигурност действително функционират, например проверка на работата на антивирусната програма и дали тя наистина предпазва вашите системи от заплахи, както и дали предоставя защита срещу нови заплахи, които първоначално не са били взети предвид. За изпълнението на тази стъпка отново трябва да назначите лице, което да отговаря за нея (например отделът за информационна сигурност във вашата организация или пък друга компания, която работи в сферата на информационната сигурност).

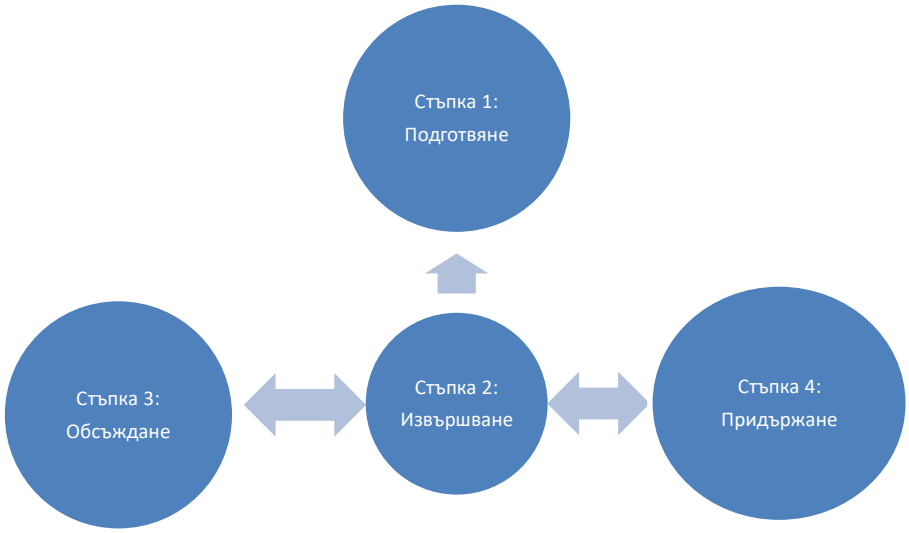
Стъпка 5: Нека предположим, че вече сте установили наличието на риск, какви действия ще предприемете за намаляването му? Нещо повече, възможно ли е прилагането действията, които смятате за подходящи? Има ли причина, поради която бихте приели наличието на определен риск (в случай, че сте оторизиран да извършвате такива действия), например дадени антивирусни програми не могат да бъдат инсталирани на местата на терминалите за продажба? Какво ще направите в такъв случай, ще приеме риска да нямате антивирусен софтуер или ще потърсите друго компромисно решение? За изпълнението на тази стъпка отново ще трябва да определите отговорно лице или лица (например отделът за информационна сигурност във вашата организация).

Стъпка 6: Последната стъпка на жизнения цикъл на този процес се състои в продължителното наблюдение на информационната система, приложените мерки за сигурност и степента на тяхната ефективност. Често използван метод представлява регистрирането на всяко едно действие на системата, пакетите на мрежовия трафик, системните транзакции, потребителските сесии и други. Това се прави, тъй като регистрирането ще ви помогне да наблюдавате и установявате различните рискове или нарушения на цялата система, като преглеждате регистрираните файлове. Този процес позволява да се предприемат незабавни действия, когато това е нужно. При неговото изпълнение също е нужно да назначите лице или лица, които да го контролират (например специалисти в областта на домейните, които са служители във вашата организация) [33].

Избирането на подходяща Рамка за Управление на Риска изисква внимателно обмисляне, защото впоследствие вие ще имате нужда от една цялостна рамка, която ще подпомага развитието на вашата бизнес среда.

Значителна роля в Рамката за Управление на Риска има **Оценката на Риска**. Процесът по оценка на риска се състои от няколко стъпки: подготвяне на оценката, извършване на оценката, обсъждане на резултатите от оценката и

придържането към нея. Тези стъпки са илюстрирани във Фигура 2, където е развит и процесът по Оценка на Риска.



Фигура 2: Оценка на риска [34]

Стъпка 1: Подготвяне на оценката. Първо, установете каква е целта на извършваната оценка. Помислете за нещата, които оценката се стреми да обхване; за това какъв е нейният обхват. Предположенията и ограниченията във връзка с оценката следва да бъдат определени. Нещо повече, източниците на информация, които ще използвате за извършване на оценката, следва да бъдат посочени. Последното действие се изразява в определянето на рисков модел и на различните подходи.

Стъпка 2: Извършване на оценката. Разгледайте различните източници на заплаха и евентуалните събития, които могат да се породят от последните. След това определете уязвимостите във системите на вашата организация, като това ще ви помогне за съставянето на специфичен план за действие при настъпване на някои от заплахите или за условия, които предразполагат настъпването на такива заплахи. На следващо място, вероятността установени източници на заплаха да

доведат до нарушения на сигурността трябва да бъде определена, като следва да се предполага, че тези нарушения ще се осъществят. Страничните ефекти следва също да бъдат определени; влиянието върху организационните операции и активи, лицата, други организации, включително и на национално ниво. Това може да бъде причинено от възползването от уязвимостите посредством източниците на заплаха чрез определени заплашващи събития. Нужни са разяснения затова кои рискове за сигурността могат да бъдат част от комбинация на възможните заплахи и уязвимости, както и за евентуалното тяхно влияние, включително влиянието на всякакви несигурности, свързани с определянето на риска.

Стъпка 3: Обсъждане на резултатите. Резултатите от оценката следва да бъдат добре разбрани и осмислени. След като бъдат разбрани, вие можете да споделите с другите информацията, която е използвана като отправна точка в началото на изследването. При обсъждането на резултатите, вие можете да поддържате и прилагането на други дейности за оценка на риска.

Step 4: Придържане към резултатите. Рисковите фактори, които са определени при оценката на риска, трябва да бъдат наблюдавани продължително, за да проучим наличието на всякакви последващи техни промени. Не забравяйте да обновявате компонентите на оценките на риска, така че те да дават отражение върху наблюдаването на дейностите, извършвани от вашата организация [34].

Е. Списък за Оценка на Рисковете за Дигиталната Сигурност

	✓
Стъпка 1: Подготовка за Оценка на Риска	
Установете целта на оценката	
Установете обхвата на оценката	
Установете предположенията и ограниченията, които са свързани с оценката.	
Определете източниците на информация, които ще бъдат използвани като отправна точка при оценката	
Установете рисков модел и аналитичните подходите, които да се приложат при оценката	
Стъпка 2: Извършване на Оценка на Риска	
Определете съответните източници на заплаха	
Установете заплашващите събития, които могат да се породят от източниците на заплаха	
Определете уязвимостите в организацията, които могат да бъдат използвани от източниците на заплаха чрез тези заплашващи събития, както и предразполагащите условия, които могат да повлияят на извършването на оценката	
Определете каква е вероятността установените източници на заплаха да породят особени заплашващи	

сигурността събития, както и вероятността тези заплашващи събития да се породят успешно	
Определете вредните влияния върху операционните дейности и активите на организацията	
Установете рисковете за дигиталната сигурност като комбинация от вероятността за възползване на заплахите от уязвимостите и влиянието на такова възползване.	
Стъпка 3: Обсъждане и обмен на информацията относно Оценка на Риска	
Обсъдете резултатите от оценката на риска	
Споделете събраната информация при извършването на оценката на риска	
Стъпка 4: Придържане към оценката	
Наблюдавайте рисковите фактори, които установите при оценката на риска, като вземате последните предвид при извършването на бъдещи оценки	
С оглед на последващи промени в рисковите фактори, обновявайте редовно елементите на оценките на риска в зависимост от тяхното значение за наблюдаваните дейности [34]	

F. Терминологичен речник

Риск – потенциалната възможност за загубване на нещо значимо [35].

Оценка на риска – процесът по установяване на рискове, които са свързани с определена ситуация, както и по определяне на вероятността от настъпване на тези рискове и техните евентуални последици, и процесът по осигуряване на допълнителни мерки с цел ограничаване на последиците. Оценката на Риска представлява част от процеса по Управление на Риска, като Анализирането на Риска се използва като синоним [34].

Управление на риска – цялостният процес по установяване, наблюдаване, контролиране и понижаване на рисковете. Както вече отбелязахме, този процес включва в себе си и процеса по Оценка на Риска [34].

Заплаха – потенциалната възможност за източника на една заплаха да се възползва от определена уязвимост [34].

G. Заключения и допълнителна информация

След прочитането на настоящото ръководство, вие вече имате представа затова колко точно е важно прилагането на Оценката на Рисковете за Дигиталната Сигурност за цялостните процеси по управление на риска и вземане на управленски решения във вашите организации. В настоящата глава ви представихме пълен преглед на възможните подходи при Оценка на Рисковете за Дигиталната Сигурност, които потенциалните и настоящи млади предприемачи трябва да спазват в своите бизнес начинания, включително при въвеждането на стратегии за извършването на тези оценки в своите организации. С оглед на гореизложеното, надяваме се да сме изпълнили пълноценно нашата цел, която се изразява в обогатяването на знанията на младите предприемачи, както по отношение на техническите аспекти (Дигиталната Сигурност като Технически Риск), така и по отношение на икономическите аспекти (Дигиталната Сигурност като Икономически Риск) на Дигиталната Сигурност.

В заключение, следва да препоръчваме преглеждането на допълнителна информация от други източници по темата, които знания биха подпомогнали цялостното разбиране на материята.

Н. Източници

[1] http://searchcompliance.techtarget.com/definition/risk-assessment, access 13.11.2017

[2] https://www.mindtools.com/pages/article/newTMC_07.htm, access 13.11.2017

[3] http://www.genre.com/knowledge/blog/steps-to-a-good-risk-assessment-en.html, access 13.11.2017

[4] https://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security, access 13.11.2017

[5] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm, access 13.11.2017

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport, access 27.01.2018

[7] https://www.lifewire.com/what-is-malware-2625933, access 27.01.2018

[8] https://oit.ncsu.edu/it-security/safe-computing/viruses/, access 16.05.2018

[9] https://www.trendmicro.com/vinfo/us/security/definition/address-bar-spoofing, access 16.05.2018

[10] https://www.acunetix.com/websitesecurity/cross-site-scripting/, access 27.01.2018

[11] https://www.lastline.com/blog/drive-by-download/, access 16.05.2018

[12] https://searchsecurity.techtarget.com/feature/Targeted-Cyber-Attacks, access 16.05.2018

[13] https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf, access 16.05.2018

[14] https://www.sans.org/reading-room/whitepapers/application/web-browser-insecurity-1637, access 16.05.2018

[15] https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053, access 16.05.2018

[16] https://www.business.att.com/learn/operational-effectiveness/the-top-10-web-application-security-risks.html, access 16.05.2018

[17] http://www.trendmicro.it/media/misc/web-application-vulnerabilities-en.pdf, access 16.05.2018

[18] http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-a-risk-damages-from-phishing/#gref, access 16.05.2018

[19] https://www.bloxx.com/media/1356/bloxx_whitepaper_increasingemailthreats_us.pdf, access 17.05.2018

[20] https://www.techsoup.org/support/articles-and-how-tos/things-you-can-do-to-prevent-spam, access 17.05.2018

[21] https://www.facebook.com/help/217854714899185, access 17.05.2018

[22] https://www.quora.com/How-dangerous-is-a-DDoS-attack, access 17.05.2018

[23] https://www.computerweekly.com/feature/DDoS-attack-threat-cannot-be-ignored, access 17.05.2018

[23] https://www.computerweekly.com/feature/DDoS-attack-threat-cannot-be-ignored, access 17.05.2018

[24] https://www.veracode.com/security/botnet, access 17.05.2018

[25] https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats/, access 17.05.2018

[26] https://www.kroll.com/en-us/what-we-do/cyber-security/prepare-and-prevent/cyber-risk-assessments/data-breach-prevention-tips, access 17.05.2018

[27] https://www.privacyrights.org/consumer-guides/how-reduce-your-risk-identity-theft, access 17.05.2018

[28] https://www.thebalance.com/prevent-identity-theft-1947624, access 17.05.2018

[29] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, http://dx.doi.org/10.1787/9789264245471-e, p. 9

[30] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, http://dx.doi.org/10.1787/9789264245471-e, p. 19-20

[31] OECD, Managing Digital Security and Privacy Risk for Economic and Social Prosperity, OECD Publishing, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2016)1/FINAL&docLanguage=En, p. 14-15

[32] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, http://dx.doi.org/10.1787/9789264245471-e, p. 35

[33] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf, access 11.06.2018

[34] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, access 11.06.2018

[35] https://en.wikipedia.org/wiki/Risk, access 11.06.2018

Благодарствена бележка от екипа на DiFens

Надяваме се настоящото електронно ръководство да ви послужи при навлизането в света на дигиталната сигурност, като подпомогне развитието на вашите настоящи и бъдещи предприятия, насочвайки вашите възможности в правилната посока.

Чувствайте се свободни да си набавите допълнителна информация по темата от всички горепосочени допълнителни източници, както и чрез запознаването с друга допълнителна литература, която да съответства на потребностите на вашата организация.

Ако имате нужда от допълнителна информация, не се притеснявайте да потърсите такава на платформата за обучения на DiFens, която е достъпна на страница http://www.difens.eu/ . Щом веднъж се почувствате достатъчно уверен, вие можете да станете ментор в нея и да помагате на други млади предприемачи в техните начинания чрез споделяне на вашите знания и опит с тях.

За повече информация относно проекта и екипа, които стои зад него, моля посетете http://difens-project.eu/ или се свържете с нас на difensproject@gmail.com .

Благодарим Ви за отделеното внимание и Ви пожелаваме успех при осигуряването на подходящите защитни мерки за вашата организация!