СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Проект “Интеррегионално насърчаване на социалните предприятия”
„Interregional Social Enterprise Empowerment”,
с акроним I SEE се финансира по договор за безвъзмездна помощ
B2.9c.06 от 23.10.2017г., по програма ИНТЕРРЕГ V-A
Гърция - България 2014-2020

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

МОДУЛ 3 – ЗАЩИТА И ПОВЕРИТЕЛНОСТ НА ДАННИ

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

1. МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

- Компютърна сигурност- Защита на компютрите, информацията, която се намира на тях и услугите от неоторизиран достъп, промяна или унищожаване.
- Мрежова сигурност- допълва концепцията на компютърната сигурност до свързаните до тях системи:
  - Интернет браузване
  - Електронна търговия
  - Социални мрежи
  - Мейл

Компютърната и мрежова сигурност е свойство на компютърните системи и мрежи да противодействат на опитите за несанкциониран достъп до обработваната и съхраняваната информация, водещи до деструктивни действия и получаване на лъжлива информация.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Сигурността е свойство на една система да противостави на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение. Това важи и за сигурността на информационните системи.

• Целта на всяка информационна система е предоставяне на пълна, достоверна и своевременна информация. Тази информация е уязвима както поради случайни, така и поради злонамерени дестабилизиращи фактори (заплахи), което налага да се вземат мерки за нейната защита.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Какво представлява защита на информацията
• постоянно използване на средства и методи, прилагани с цел:
• а) защита на конфиденциалността (тайната) - да не се допуска разкриването на информация от неоторизирани лица;
• б) защита на цялостността - да не се допуска неоторизирана преднамерена или случайна модификация на информацията;
• в) защита на достъпността - да не се допуска отказ на информация или ресурс.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

2. ВИДОВЕ ЗАПЛАХИ

В кибер- пространството гъмжи от различни видове заплахи:

- Компютърни вируси; Троянски коне; Кражба на контакти; DNS Отравяне; Зомбита, IP измама; Грабеж на парола; Логически бомби; Мрежови червеи; Отвлечени начални страници; Атаки за отказ от услуга; Препълване на буфера; Разбиване на пароли.

- Според **източника** заплахите могат да бъдат външни и вътрешни.
  - **Външни** са дейността на разузнавателни и специални служби, дейността на разни политически, икономически и други структури, насочени срещу интересите на организацията, и престъпни действия на отделни групи и лица.
  - **Вътрешни** са нарушаване на правилата за събиране, обработка и предаване на информацията, незаконна дейност на групировки и лица за прикриване на закононарушения и нанасяне на вреди на интересите на физически и юридически лица на базата на тази информация.

Видове заплахи според **произхода** на заплаха:

• **Естествените** са заплахи от обективни физически процеси или стихийни природни явления, независещи от човека - пожари, наводнения, урагани, земетресения и нарушения в инфраструктурата (аварии в електрозахранването, аварии в системите за връзка, прекъсване на водоснабдяването и т.н.).

• **Изкуствените** заплахи са предизвикани от действията на хора. Те биват непреднамерени (неумишлени, случайни) и умишлени. Според статистиката около 65% от щетите, нанесени на информационните системи, са следствие на непреднамерени грешки, а само 13% на стихийни бедствия и аварии.

Interreg
Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

Два вида защита на данните

- а) защита от разрушаване, която включва: антивирусна защита, контрол за автентичност на данните и програмите, защита от хардуерни и софтуерни грешки, защита от грешки на персонала;
- б) защита от нерегламентирано ползване, която включва: контрол и регламентиране на достъпа до данните и криптографска защита на данните.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

3.НОРМАТИВНА БАЗА

• Както във всички развити страни, така и в нашата страна системи за компютърна сигурност са въведени предимно в държавните организации. Нормативната база за тях са редицата приети документи :

• Закон за защита на класифицираната информация;

• Закон за достъп до обществената информация;

• Когато информационните системи обработват класифицирана информация, те трябва да отговарят на изискванията на приетата от Министерския съвет.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Нормативна уредба на системата за защита

- "Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация"
- На 17 ноември 2008г. със постановление № 279 Министерски съвет прие Наредба за общите изисквания за оперативна съвместимост и информационна сигурност към Закона за електронното управление.
- В допълнение към другите изисквания към администрацията в Наредбата е посочено и изискването в 12 месечен срок след публикуването и всички административни структури да са сертифицирани по ISO 27001 – международния стандарт за системи за управление на информационната сигурност.

Interreg
Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

4. НАЧИНИ И СИСТЕМИ ЗА ЗАЩИТА НА ДАННИТЕ

Защо трябва да управляваме риска?

- Управлението на риска се превръща в значим управленски процес, който има решаващо значение за вземането на обосновани, обективни решения с по-висока степен на определеност.
- Увеличава вероятността за постигане на организационнните цели -печалба, приходи, пазарен дял
- Разкрива слабостите и уязвимостта
- Разширява възможностите за успех
- Повишава доверието на заинтересованите (акционери, менидж.)

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Какво е риск?

Понятието „риск” (от латинската дума risico –„опасност”, „несигурност”) е решение, начинание или постъпка, резултатът от които е неизвестен. Рискът се определя като „отклонението от един или повече резултати на едно или повече бъдещи събития от тяхната очаквана стойност”.

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

Видове риск:

- Интегрален и частен;
- Риск от 1 и 2 род;
- Стратегически, организационен и оперативен;
- Политически, социален, икономически, управленски, физически, екологически, персонален;
- Присъщ и привнесен.

Икономически риск:

- Пазарен;
- Финансов;
- Банков;
- Инвестиционен;
- Секторен (търговски; логистичен; транспортен; индустриален; енергиен...)
- Корпоративен;
- Фирмен.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

Корпоративен риск:

- Извънреден или застрахователен (пожар; кражба; бедствие; прекъсване; замърсяване; пенсионен);
- Финансов (лихвен; обменен; капиталов; ликвиден; кредитен);
- Оперативен (задоволеност; продуктов; търговска марка; лидерски; IT; кражба);
- Стратегически (качество; предпочитания; иновация; регулация; политически).

Interreg
Greece-Bulgaria
European Regional Development Fund

EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

5. ИДЕНТИФИКАЦИЯ И АВТЕНТИКАЦИЯ

• Идентификация е един или няколко ИТ метода които използва крайният потребител (човек или компютър) за да се обособи и различи от другите крайни потребители в ИТ системата. Идентификационния ИТ метод определя как крайния потребител да се обособи и различи.

• Автентикация е един или няколко ИТ процеса установяващи валидността между крайния потребител и неговата претендирана самоличност. Автентикацията използва един или няколко фактора, посредством които ИТ процесите извършват проверка на достоверността на крайния потребител.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

Автентикационният фактор

• Автентикационният фактор е информация или устойство– например парола, Цифров сертификат, Смарт карта, Биометрични данни и т.н.
• Един или няколко идентификационни метода може да изискват един или няколко автентикационни ИТ процеса използващи един или няколко фактора за автентификация.
• Един фактор за автентикация може да участвува в един или няколко метода за идентификация.

Фактор за автентикация

- В световната практика е прието първият фактор за автентикация да е с класификацията „да знаеш нищо”, например като ПИН код, парола, и т.н.
- Прието е също така вторият фактор за автентикация да е с класификацията „да имаш нещо”, например смарт карта, USB интелигентно устройство, мобилен телефон по който да получиш допърнителна парола, и т.н.
- Често в световната практика се използват биометричните данни като трети фактор за автентикация, например отпечатък на пръст, форма на лицето, изображение на ириса, и т.н.

Методи за автентикация

А) Отворен фактор – не се изисква никаква форма на автентикация;
Б) Фактор „Нещо което знае потребителя” – Потребителят знае своето потребитеско име и парола за достъп до уеб страница;
В) Фактор „Нещо което има потребителя” – използва се смарт карта вградена в USB носител с инсталирана двойка частен и публичен ключ, заедно с цифров сертификат;
Г) Фактор „Нещо което знае потребителя и нещо което има потребителя” – използва се смарт карта четец с ПИН клавиатура и смарт карта със защитни ключове;
Д) Фактор „Нещо което представя потребителя и нещо което има потребителя” – използва се смарт картов четец със скенер за биометрични пръстови отпечатъци и смарт карта със защитни ключове.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

6.КРИПТОГРАФИЯ

Криптография - един от най- разпространените методи за защита на информацията при предаването на данни в компютърните мрежи и предимно при обмен на информация в свързочни канали между отдалечени обекти.

- Шифър – математически алгоритъм за криптиране (декриптиране) на информация;
- Криптиране – превръщане на открития текст в скрит, използвайки даден шифър (алгоритъм);
- Декриптиране – превръщане на скритият текст в явен (обратният процес на криптирането);

Компоненти на криптографията

• открит текст (plaintext, cleartext) - входните данни за криптографския алгоритъм;
• шифротекст (ciphertext) - изходните преобразувани данни.
• Наричат се още криптограма (cryptogram) или шифрограма (ciphergram);
• шифриране или криптиране (encryption) - процеса на преобразуване на открития текст в криптограма;
• дешифриране или декриптиране (decryption) - процеса на преобразуване на една криптограма в открит текст;

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Криптоалгоритъм

• Криптоалгоритъм се счита за напълно стабилен, ако прочетете шифрования блок от данни и преминавайки през всички възможни ключове съобщението няма смисъл.

• В теорията на вероятностите, желаният ключ може да бъде открит с вероятност 1/2 след итерацията през половината от всички клавиши.

• По този начин, като цяло стабилността на блоковия шифър зависи само от дължината на ключа и нараства експоненциално с нарастването му.

• Дори и да се предположи, че търсенето на ключове се извършва на специално създадена многопроцесорна система.

Класификация на алгоритмите

• Симетрични (със секретен ключ)– криптиращият и декриптиращият ключ са едни и същи. И предавателят и приемникът знаят ключа.

▫ Симетрични са : Цезаров шифър, Шифър на Вижънър и др.

• Асиметрични (несиметрични, с публичен ключ) – криптиращият и декриптиращият ключ са различни. Предавателят знае само ключа за криптиране, а приемника само за декриптиране.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

7. РЕЗЕРВНИ КОПИЯ И ВЪЗСТАНОВЯВАНЕ НА ДАННИТЕ

ЩО Е АРХИВИРАНЕ (КОМПРЕСИРАНЕ)

- Процес, при който се създават резервни копия на данните с цел да се съхранят за продължителен период от време;
- За намаляване на размера на компресираните файлове се прилагат различни математически методи и алгоритми, при които на входните данни се съпоставят кодове по определени правила, премахват се повтарящи се символи и др.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

ЗАЩО СЕ ИЗПОЛЗВА КОМПРЕСИРАНЕ?

- За намаляване на размера на файла с цел прехвърлянето му на външен носител;
- За по-бързо предаване на данни в мрежа;
- За защита от някои вируси;
- За дългосрочно съхранение.

ПРОГРАМИ ЗА АРХИВИРАНЕ (АРХИВАТОРИ)

- Архиваторите са програми, които служат за създаване на резервно копие на данни. Сред най-популярните програми за компресиране и архивиране за Windows са WinRar и WinZip.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

ПРОГРАМИ ЗА АРХИВИРАНЕ (АРХИВАТОРИ)

•BACKUP – служебна програма на Windows за работа с компресирани файлове

•WinZip
•Win Ace
•7-Zip
•WinRar
•Power Archiver
•IzArch

Процес на АРХИВИРАНЕ

•Избиране на файл, папка или група от файлове за архивиране;
•Добавяне на файлове към архив (Добавяне или Add);
•Задаване на име и място на архива;
•Задаване на допълнителни настройки – формат на архива, ниво и метод на компресия, възможности за разделяне на томове, добавяне на парола и др.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

8. РЕГЛАМЕНТ НА ЕС 2016/679 ВЛИЗАЩ В СИЛА ГО 25 МАЙ 2018

• На 25 май 2018 г. влиза в сила нов регламент на ЕС за защита на информацията (GDPR – General Data Protection Regulation).

• Ако съхранявате каквито и да било данни за клиентите и партньорите си, трябва да се съобразите с изискванията на новия регламент.

• General Data Protection Regulation (или Общ регламент относно защитата на данните) ще засегне всяка организация в ЕС, която съхранява лични данни, както и всеки един бизнес в рамките на ЕС.

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Изискванията на ЕС за съхранение на лични данни, въведени с GDPR, са свързани с организационни и технологични мерки, както и с мерки за съхранение на информацията, вкл. въвежда се изискването определени типове организации да назначат Служител по защита на данните (DPO - Data Privacy Officer).
Организациите трябва да разполагат с подобна позиция или като член от персонала, или под формата на външен консултант.
Служителят по защита на данните ще отговаря за съобразността с изискванията на регламента, ще консултира въвеждането на нови такива и ще консултира кога и как трябва да бъде осъществено оценяване на степента на важност на личните данни. Той ще бъде и лицето за контакт с националните органи за защита на личните данни.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Основни права на притежателите на лични данни

1. Правото да бъде информиран
2. Правото на достъп
3. Правото на поправка
4. Правото да ограничи обработването
5. Правото да бъде „забравен“
6. Правото на преносимост
7. Правото да възрази
8. Права във връзка с автоматичното вземане на решения и профилиране

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

9. ВЪНШНИ РЕСУРСИ И ИЗТОЧНИЦИ НА ИНФОРМАЦИЯ.

Информацията (от на латински: informatio – разяснение, изложение, осведоменост) е понятие, свързано с обективното свойство на материалните обекти и явления (процеси) да пораждат многообразие от състояния. Терминът „информация" е тясно свързан с понятия като комуникация, система за управление, образование, значение, стимул, възприятие.

Interreg Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

I-SEE

Длъжностно лице по защита на личните данни

• Обработването се извършва от публичен орган или структура (с изключение на съдилищата);

• Основните дейности на администратора или обработващия се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни;

• Основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни.

Interreg
Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

Източници на информация

1. Публикации- Брошури и изложения; Презентации;
2. Данни;
3. Анализи- Доклади; Изследвания; Оценки;
4. Снимки- Карти; Видеоматериали; Лого и графики;
5. Правни текстове- Регламентите; делегирани актове; актове за изпълнение; Насоки; Комуникации; Решения;
6. Информационен център.

Interreg
Greece-Bulgaria
European Regional Development Fund
EUROPEAN UNION

I-SEE

СМОЛЯНСКА
ТЪРГОВСКО ПРОМИШЛЕНА ПАЛАТА

БЛАГОДАРЯ ВИ ЗА ВНИМАНИЕТО!