SoCyber

makes you feel secure

Всичко опира до това кой контролира информацията.

Кои сме ние?

- Иновативна компания за кибер сигурност с основен фокус да защитим **вашата информация.**
- **Международен екип** от експерти по киберсигурност със световен опит.
- Компания с доверени партньори в областта на **кибер застраховането, сертифицирането за съответствие и решенията за DDoS защита.**
- **Вашият** асистент по кибер сигурност.

С какво можем да сме ви полезни?

Ние ще ви накараме да се чувствате сигурни и ще защитим **вашата** информация, защото:

- Кибер атаките могат да струват **скъпо.**
- **Вашата** информация е вашият бизнес.
- **Вашата** сигурност е доверието на вашите клиенти и наша основна мисия.

Кибер пробив може да доведе до корпоративни загуби, репутационни проблеми, налагане на санкции и загуба на доверие сред клиентите и партньорите.

Директорите на компании могат да бъдат подведени под отговорност, за това че не са се погрижили за предотвратяване на щетите. Те следва да са информирани за наличните защити в корпорацията.

В светът в който живеем е въпрос на време **кога,** а не **дали** ще настъпи кибер пробив. Кибер сигурността се превръща в една от най-важните теми за бизнеса.

Каква е опасността?

- **Кибер атаките са навсякъде** – в сектора на туризма и транспорта, банковия сектор, онлайн магазини, лични данни, интелектуална собственост, търговски тайни и др.

- Компаниите могат да претърпят щети и под формата на **DDoS атаки**, които да саботират техните системи, чрез изпращане на огромно количество ненужен трафик, правейки ги недостъпни за потребителите.

- Голям брой кибер атаки **остават незасечени**, особено когато се извършват с цел **индустриален шпионаж**, където кражбата на данни може да остане незабелязана с години.

- Повечето кибер инциденти **остават прикрити**, с цел да се избегне уронване на имиджа на компанията.

Можем да проверим вашата сигурност

Тестване на сигурността за откриване и отстраняване на пропуски:

- Оценка на уязвимости
- Тестване за проникване в уеб приложения
- Тестване за проникване в мобилни приложения
- Външни тестове за проникване в мрежи
- Вътрешни тестове за проникване в мрежи

ИТ одит на сигурността на информационните системи:

- Windows устройства
- Linux устройства
- Мрежови устройства
- Персонализиран софтуер

Извършване на тестове за **социално инженерство**:

- По телефона (vishing)
- По имейл
- SMS съобщения

Можем да бъдем вашият доверен консултант по сигурността

Мрежи

- Защитни стени
- WAF
- IPS/IDS
- SIEM решения
- Honeypots
- DLP решения
- Windows сигурност
- Linux сигурност
- Proxy сървъри

Приложения

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting
- Insecure Decentralization
- Known Vulnerabilities
- Insufficient Logging

Принципи и политики

- Процедури
- Насоки
- Стандарти
- Политики

И можем да обучим вашите служители

- Пароли
- Политики за сигурност
- Резервен план
- Социално инженерство
- Сигурно използване на уеб
- Реакция при инцидент
- Криптиране
- Посетители
- Индивидуалност на служители
- Практически демонстрации

Защо GDPR е толкова важен?

Нарушенията могат да доведат до глоби, по-големи от **20 милиона** евро или **4%** от общия брутен оборот на предприятието.

Дава възможност на лицата да контролират по-добре своите лични данни с един единствен набор от правила.

Регламентът задължава **администраторите** да ангажират само **обработващи** данни, които отговарят на изискванията на Регламента, и защитават правата на субектите на данни.

"**Лични данни**" - всякаква информация, свързана с лице, което може да бъде идентифицирано пряко или непряко (име, идентификационен номер, данни за местоположението, онлайн идентификатор или фактори и други.)

Изисквания на GDPR

Основни

Обработката на данни за **"цели на директен маркетинг"** може да се счита за легитимен интерес.

Всички компании и органи на публичната администрация, които са администратор или обработват лични данни трябва да назначат **отговорник по защита на данните**.

Подход, основан на риска - да бъде разработен съответният контрол на организацията в зависимост от степента на риска, свързан с дейностите по обработката на данни.

В случай на изтичане на лични данни, администраторите на данни **трябва да уведомят съответния надзорен орган**, без забавяне и не по-късно от 72 часа.

Изисквания на GDPR

Технически

Процес за **редовно тестване, оценка и проверка** на ефективността на техническите и организационни мерки за гарантиране на сигурната обработка.

Способността да се **гарантира непрекъснатата поверителност, целостта, достъпността и устойчивостта** на системите и услугите, обработващи лични данни.

Възможността за **своевременно възстановяване на наличието и достъпа до данни** в случай на физически или технически инциденти.

Необходима е **псевдонимизация и/или криптиране** на личните данни.

Защита на данните по време на **обработката, прехвърляне и съхранение**.

Защита чрез засичане на атаки

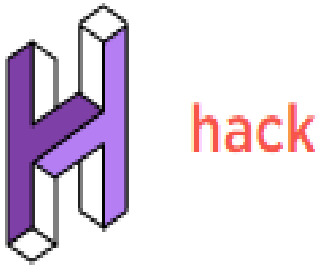
Отговор при инцидент

- Разработване на система за мониторинг и идентифициране на потенциални заплахи.
- Подгответе се за възстановяване на бизнеса в случай на атака.
- Анализирайте тежестта на заплахата и уведомете властите в рамките на 72 часа.

DLP решения

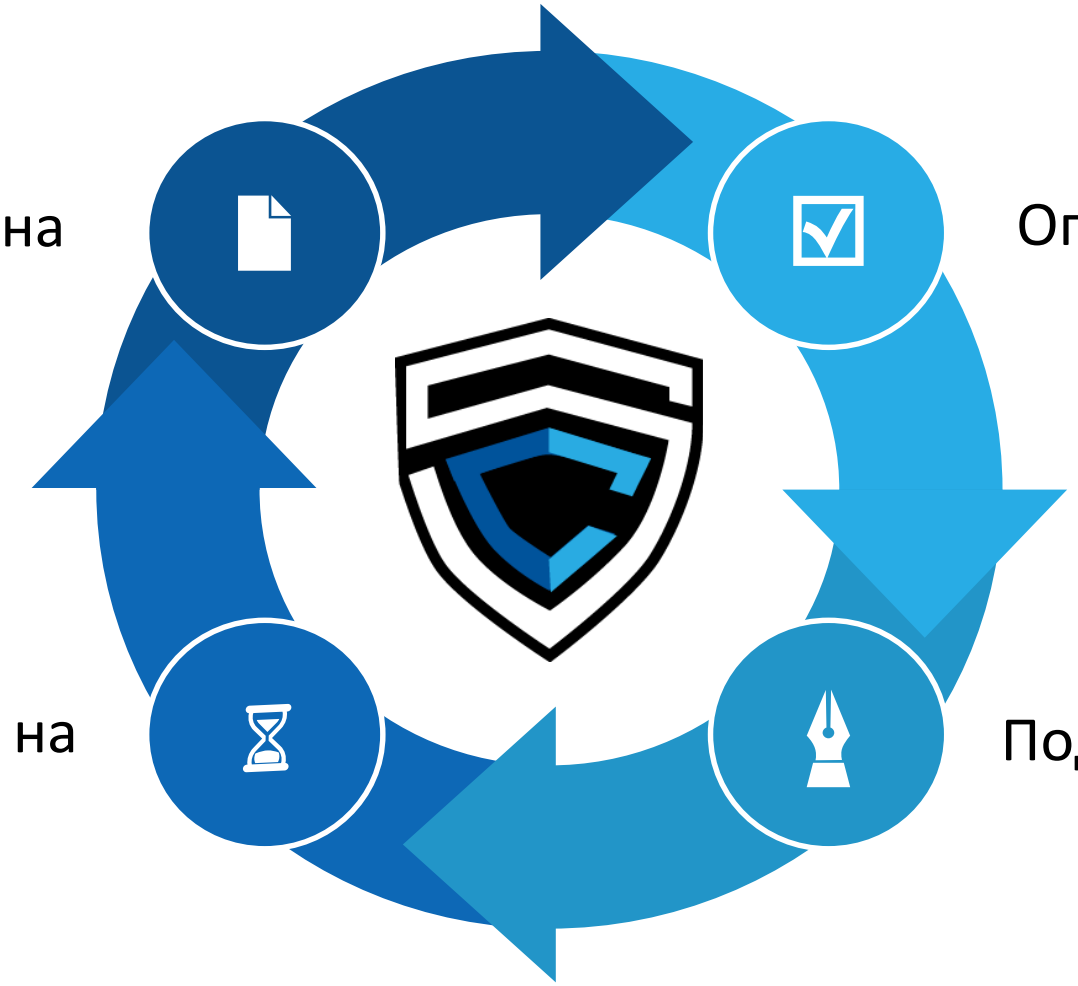
- **Мрежови DLP решения –** Анализиране на трафика за чувствителни файлове по време на предаване - имейл комуникация, съобщения, социални мрежи, уеб приложения, SSL трафик и др. Анализите се основават на предварително дефинирани политики за сигурност.
- **DLP решения за съхранение –** Анализиране на информацията в бази данни, решения на SharePoint и файлови сървъри.
- **DLP решения за крайни устройства** - Интегриране на работни станции, лаптопи, таблети и т.н. и може да се проследява информация на диск и носители на Flash Drive, webmail, социални медии, USB и др. Администраторът има право да блокира конкретни действия.

Нашите партньори

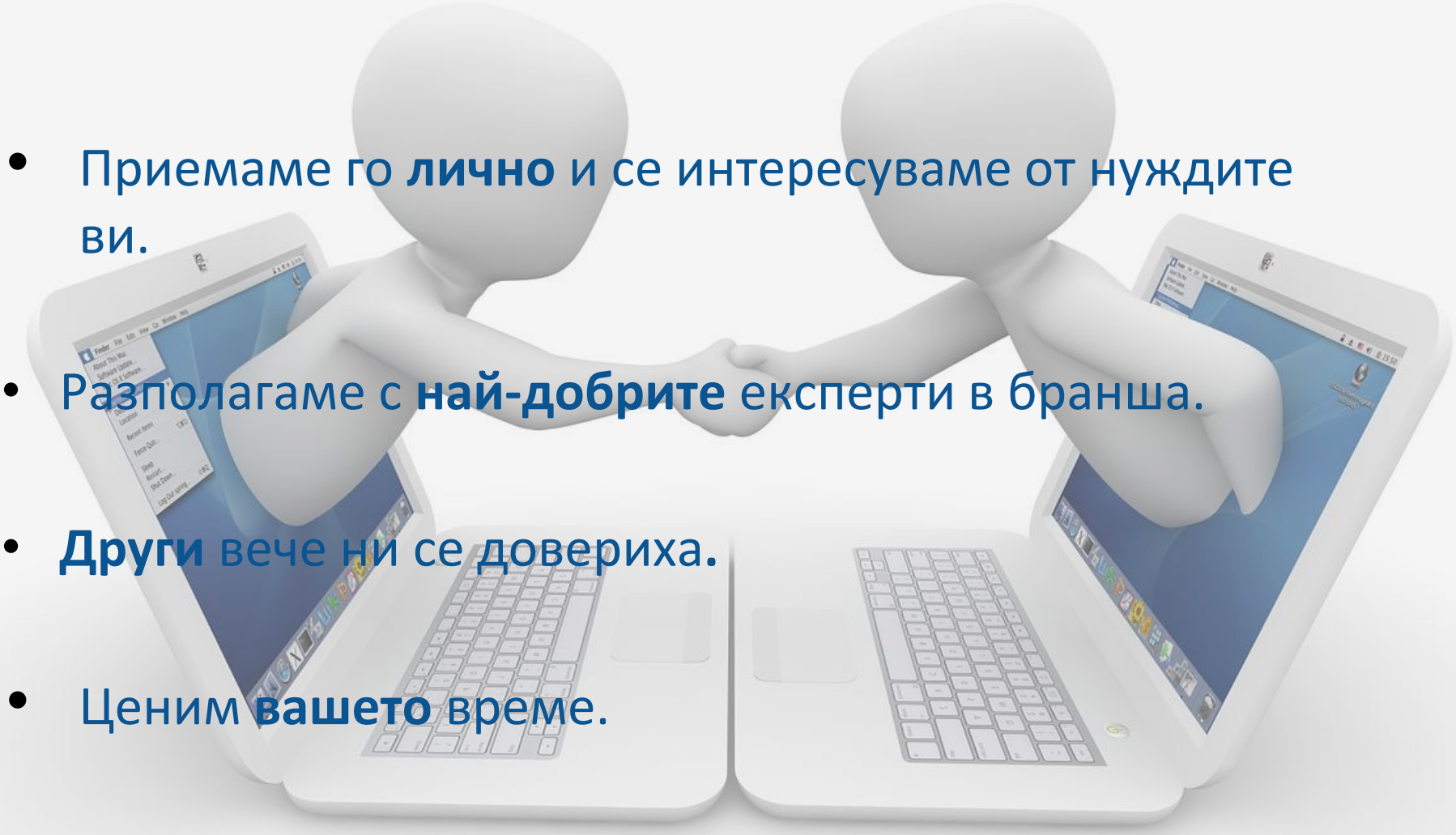


Нашите клиенти

Лесно е!


Получаване на доклад
Определяне на обхвата
Извършване на услугата
Подписване на договор

Защо нас?



- Приемаме го **лично** и се интересуваме от нуждите ви.
- Разполагаме с **най-добрите** експерти в бранша.
- **Други** вече ни се довериха**.**
- Ценим **вашето** време.

SoCyber
makes you feel secure

Искате ли да научите повече?

С удоволствие ще се срещнем с вас.

office@so-cyber.com

www.so-cyber.com

+359 876 761 555