Разпит на свидетел А.И.

Аз съм собственик на дружеството **** ООД. Дружеството се занимава с известяване на бизнес клиенти на фирми. Сайтът на дружеството е ******.bg. Данните от сайта се съхраняват на компютърна конфигурация собственост на фирма за предоставяне на хостинг услуги. Изграждането и поддръжката на сайта се осъществява от служител на дружеството. В сайта на дружеството се съхраняват чувствителна информация, имам предвид данни за клиенти – име на фирма, булстат, телефон за връзка, адрес, банкова сметка, фактури към клиенти, суми за плащане. Искам да поясня, че нашите клиенти влизат в сайта ******.bg посредством име и парола, след което чрез сайта изпращат съобщения до техни клиенти. Съобщенията, които изпращат могат да бъдат SMS или вайбър.

По време на разпита ми беше предявена експертна справка №****

По отношение на предявените материали мога да кажа, че това са файлове, в които се съдържа чувствителна информация за клиенти, които са част от базата данни на дружеството, които пък се съхраняват в сайта на дружеството ******.bg. В папката „backDB“ се съдържат следните файлове: blackList**********.***, company.***, credit_debit_invoice.***, globalSettings.***, paypalPayments.***, phonebook.***, users.***, users_bitcoin.***, users_copy.***, usersSettings.***, usersVas.***, както и други файлове. Искам да поясня, че наименованието на файловете в предявената ми експертна справка са абсолютно идентични с наименованието на файловете в базата данни на дружеството.

Първият файл blackList********.*** съдържа данни за клиенти и техните телефонни номера, до които не трябва да се изпращат съобщения. В цитираната папка са обобщени всички клиенти и техните телефонни номера, като това са клиентите на нашите клиенти.

Вторият файл company.*** съдържа също информация за клиенти, до които не трябва да се изпращат съобщения.

Третият файл credit_debit_invoice.*** съдържа кредитни и дебитни известия към фактури на фирма ****, които се издават към нашите клиенти. Имаме система за фактуриране и там се генерират фактурите към клиентите, кредитните и дебитните известия, като кредитните и дебитните известия се съхраняват в този файл.

По време на разпита ми беше предявена експертна справка № ****, като по отношение на съдържанието на файл credit_debit_invoice.*** категорично заявявам, че е абсолютно идентично със съдържанието на нашата база данни. Това е част от нашата база данни и представляват информация за кредитни и дебитни известия към фактури на клиенти на дружеството.

Във файлът globalSettings.*** се съхраняват имейли на служители на дружеството, които следва да бъдат известени при проблем с компютърната система на дружеството.

В paypalPayments.*** се съхраняват на данни за всички опити за плащане от страна на клиентите ни.

В phonebook.*** се съдържат имена и телефонни номера на клиентите на нашите клиенти.

Следващият файл users.*** съдържа информация за потребителските имена и паролите на всички наши клиенти, чрез които те използват нашия сайт. Ние записваме потребителските имена и паролите на нашите клиенти и те се запазват именно в тази папка. Това е доста чувствителна информация, тъй като дава пълен достъп до профила на конкретния клиент.

В следващия файл users_bitcoin.*** би трябвало да се съдържат данни за плащания с биткойн. Това обаче беше само тестова система и в папката реално не се съдържа информация, с изключение на една тестова транзакция. В експертната справка, от която ми беше предявена се съдържа именно тази тестова транзакция, за която категорично заявявам, че е част от базата ни данни и има идентично съдържание.

Във файла users_copy.*** съдържанието е идентично със съдържанието на users.***. Този файл всъщност представлява копие на users.***.

В следващият файл usersSettings.*** няма никакво съдържание. Това е празна таблица.

Последният файл usersVas.*** съдържа празна таблица.

По-подробна информация какво точно е съдържанието на тази папка и файловете в нея би могъл да даде служителят, който поддържа сайта. При всички положения тази информация представлява част от базата данни на дружеството, която не се намира в публичното пространство и е собственост на дружеството.

Категорично заявявам, че ние, имам предвид дружеството не сме предоставяли гореописаната информация на Тад Груп ЕООД. Нямаме сключен договор с Тад Груп ЕООД по отношение на информационната сигурност на дружеството. Не познавам собственика на Тад Груп ЕООД или техни служители. Служители на Тад Груп ЕООД не са влизали в контакт с нас.

Разпит на свидетел Р. П.

На 25.07.2018г. около 11.00 часа Отделът за поддръжка на клиенти на дружеството **** ми препратиха имейл, който са получили на **********.bg. Писмото беше изпратено от todorov_i@tad.group, беше подписано от Иван Тодоров /Ivan Todorov, Founder/, като след името се виждаше логото на ТАД Груп, адресите на фирмата и мобилен телефон. В цитираното писмо беше посочена уязвимост в сайта на дружеството - ****.bg от тип XSS. При успешно експлоатиране на този тип уязвимост има възможност за изпълнение на външен javascript и придобиване на session cookie на потребител в сайта. Имам предвид, че използването на сайта на дружеството в пълната му функционалност изисква регистрация. След като потребителят се регистрира успешно, има възможност да влиза в сайта с посочения при регистрацията имейл и парола. Успешното експлоатиране на този тип уязвимост, посочен в имейла на Тад Груп, дава възможност на трето лице да влезе в сайта с чужд профил и да придобие данните, дадени от клиента при неговата регистрация. В писмото Тад Груп ни обясняваха, че с тази уязвимост могат да крадат данни на клиентите и да се достъпи до администрацията на сайта. Освен това бяха изпратили примерен линк, чрез който демонстрираха как може да се вгради javascript код в сайта. Писмото им завършваше с предложение за съдействие от тяхна страна.

****
****
****
****

Искам да поясня, че до този момент не бях чувал за Тад Груп, не сме се свързвали с тях и не сме се договаряли да извършват подобни тестове на сайта. Дружествата **** АД и **** ООД нямат никакви правоотношения с Тад Груп.

Още същия ден написах технически обоснован отговор и го изпратих до отдела за поддръжка на клиенти, който да го препрати до Тад Груп.

След около час получих ново писмо от Тад Груп, подписано от г-н Иван Тодоров. Във второто писмо Иван Тодоров потвърждаваше нашата техническа обосновка и факта, че написаното в първия имейл няма как да се случи. Въпреки необоснованите твърдения в първия имейл, във второто писмо отново ни предложиха провеждане на цялостен тест за сигурност на сайта, чрез подписване на договор и споразумение за конфиденциалност, без финансов ангажимент.

Не проявихме интерес към направеното предложение и изобщо не отговорих на второто писмо на Тад Груп, с което комуникацията ни приключи.

От горепосочените писма става ясно, че представител на Тад Груп е извършил тест за сигурност на сайта на дружеството – ****.bg, категорично без нашето знание и съгласие очевидно, с цел да си натрапят услугите и да сключим договор за провеждане тестове за информационна сигурност с Тад Груп.

Разпит на свидетел Р.И.

По случая ще кажа следното:

От около 3 години работя в ***** на длъжност „Ръководител информационни технологии“. Предмета на дейност на фирмата е застрахователен брокер – застраховките ни са „****“, “****“, „****“ и др. Собственик на фирмата ****. Централният офис се намира в ****, където работя и аз. В моите задължения се включва инсталация на софтуер, хардуер, създаване на достъпи, сигурността на компютърните системи.

**** е регистрирана през ……..г, фирмата има сайт от доста години, домейна е ****. същия е обновяван през годините. Поддържа се от външна фирма ****. Поддръжката на сайта като структура, а актуализирането на данните в сайта го правя аз и моите колеги П.Б., която е секретар във фирмата. Самият сайт дава информация за предлаганите от нас продукти на клиенти, адрес, контакти на офисите, работно време и информационни статии свързани със застраховки и застраховането като цяло, има и калкулатор за «Гражданска отговорност» с който обикновен посетител на сайта може дори без да си прави регистрация да изчисли колко ще му струва гражданската отговорност, като въведе, модел марка на автомобила, обем на двигателя, мощност, регистрационен номер като населено място /първите две букви/, възраст на собственика / не е задължително за въвеждане/ не се въвеждат негови лични данни.

Тази година на 23.04.2019г от **** добавиха сертификат SSL за сигурност, за да не изтичат данни на фирмата. Това стана онлайн от служител на ****. Аз не познавам служителите на тази фирма, комуникираме си по имейл или телефон **** и тел. ****. Разговаряла съм с различни служители. Базата данни на сайта ни ****, се намира на виртуален сървър на фирмата ни, който се поддържа от ****. Поддръжката на сайта ни от моя страна се изразява в качване на новите тарифи и информационни статии. Сертификата за сигурност след като бъде инсталиран от **** се променя наименованието на сайта същия вече е изписан като – **** добавено е ……/. През сайта не се обработва и не се съхранява никаква лична информация дори IP адреси.

От предявената ми експертна справка №**** на стр.10, се вижда папка ****, папка **** и разширение на файл – „n_auth_ user.***“, разпознавам юзъри, които са влизали в сайта ни например „****“ , изписана е и парола, дата и час, на последно логване. Най-вероятно колежката П.Б. е влизала в калкулатора на сайта и е проверявала нещо. Юзърите „****“ не се сещам кои са. Няма как да се видят от обикновен посетител тези юзъри. Аз не съм предоставяла горните данни на Тад Груп ЕООД или на което и да е друго физическо или юридическо лице. Аз лично заедно с Т.Д. съм се срещала с представители на Тад Груп ЕООД по тяхна инициатива. Това стана на 1.04.19г. в нашия офис на ****, в заседателната зала.

Представители на Тад Груп ЕООД бяха Кристиян Бойков, който се представи като служител по Ай Ти Сигурност и още един негов колега Георги Янков, който се представи като търговски директор на Тад Груп ЕООД. Предоставиха ни презентация на тяхната фирма и с какво се занимава тя, казаха че биха могли да тестват нашата система за слабости и след това да ги отстранят, в случай, че решим да сключим договор с тях. Аз преди срещата с представителите на Тад Груп ЕООД бях избрала друга фирма с която да работим, която ни беше дала по-добра оферта. До момента все още не сме избрали фирма която да се грижи за сигурността на фирмата ни. На срещата не дадохме отговор на тяхното предложение. И двамата служители на Тад Груп ЕООД ми направи впечатление, че говорят на висок технически език. По време на презентацията разбрах, че фирмата им има главно звено в САЩ, това ми се стори несигурно. Кристиян говореше през цялото време, наблягаше на това че са правят тестове на системите. Не е казвал нищо конкретно, например с какви програми за тестване разполагат. Казаха какво може да тестват - сайт, имейли, наши служители. След провеждането на тестовете Кристиян щял да изпрати доклад, в който посочват слабостите на пробиваемите звена. Не бяха запознати с нашия технически ресурс и сайта ни. Не са говорили за конкретни цени на услугите си.

**** няма сключен договор с Тад груп ЕООД. Лицето Иван Тодоров не го познавам, от медиите научих че е собственик на Тад Груп ЕООД. Не сме правили допълнителни проверки и тестове, всичко си работи нормално.

****
****
****
****

Разпит на свидетел Б.

ВЪПРОС: Познавате ли и в какви отношения се намирате с лицата Кристиян Бойков, Георги Янков, Иван Тодоров?

ОТГОВОР: Не познавам лицата, не съм осъществявал контакт с тях. Тези лица единствено съм ги чувал от медиите във връзка с нашумелия скандал с изтекли данни от НАП.

ВЪПРОС: Моля, под формата на свободен разказ да разкажете каква е вашата професия, с какво се занимавате?

ОТГОВОР: Работя от 2015 год. като директор „Информационни технологии във фирма ****, фирмата се занимава с информационното обслужване на фирма ****.

*Предявявам на свидетеля копие от експертна справка №****, от стр.2 до 5.*

ВЪПРОС: Моля, да дадете обяснение на предявените ви материали - файл „****.txt“ от експертната справка №****, от стр.2 до 5.

ОТГОВОР: По отношение на предявените материали мога да кажа, че имената на таблиците съвпадат със такива в база данни на ****. Наименованието „dbInfoCRM“ е името на базата данни.

Тези данни се съхраняват в система, която не е достъпна в интернет пространството и без неоторизиран достъп никой не би трябвало да имат достъп до тези данни в този формат.

Данните не са публично достъпни, те са част от информационната система на дружеството и се съхраняват в сървър, който се намира във вътрешната мрежа на дружеството. До тези горепосочените данни достъп имат единствено системните администратори, които работят в „****“. Не мога да потвърдя дали числовото изражение посочено по папките е вярно.

Въпрос: Известна ли ви е фирмата „Тад Груп“ ЕООД и свързвала ли се е с вас по-някакъв повод?

Отговор:Не, тази фирма не ми е позната, както по-горе казах тази фирма ми стана известна от медиите във връзка със скандала с изтекли данни от НАП.

Въпрос: Вие предоставяли ли сте тази информация във файл „****.txt“ на фирма „Тад Груп“ ЕООД или някой от нейните служители?

Отговор: Не, не сме предоставяли тази информация. Нямаме договорни отношения с посочената фирма и същите не са извършвали одит на сигурността на IT инфраструктурата на ****.

Въпрос: Имали ли сте пробив или неоторизиран достъп до IT инфоструктурата на ****?

Отговор: Не, поне на нас не ни е известен такъв. Ако е проникнато с наш юзер нейм и парола, същият става оторизиран и на нас няма да ни е известен този достъп.

Категорично заявявам, че ние не сме предоставяли гореописаната информация на „Тад Груп“ ЕООД. Нямаме сключен договор с „Тад Груп“ ЕООД по отношение на информационната сигурност. Не познавам собственика на „Тад Груп“ ЕООД или техни служители. Служители на Тад

Груп ЕООД не са влизали в контакт с мен, като директор „Информационни технологии“.

Протокола прочетох лично и удостоверявам с подписа си, че показанията ми са записани правилно.

Разпит на свидетел М.И.

На зададените въпроси свидетелят отговори както следва: Разбирам правата и задълженията си в качеството на пострадал и свидетел, съгласно разпоредбите на НПК. Същите ми бяха подробно разяснени от водещия разследването. Не желая да ми бъдат предявени материалите по делото.

ВЪПРОС: Познавате ли и в какви отношения се намирате с лицата Кристиян Бойков, Георги Янков, Иван Тодоров?

ОТГОВОР: Не познавам лицата, не съм комуникирал с тях. Същите лица ми станаха известни от медиите преди време във връзка със скандал с изтекли данни от НАП.

ВЪПРОС: Моля, под формата на свободен разказ да разкажете каква е вашата професия, с какво се занимавате?

ОТГОВОР: Работя от 2016 год. като изпълнителен директор на ****, като дружеството се занимава със застрахователни услуги.

*Предявявам на свидетеля копие от експертна справка №****, от стр.2 до 5.*

ВЪПРОС: Моля, да дадете обяснение на предявените ви материали - файл „****.txt“ от експертната справка №****, от стр.2 до 5.

ОТГОВОР: По отношение на предявените ми материали, мога да кажа, че не съм ги виждал. Това е първия път, в който се запознавам с тях. От съдържанието на файла ****.txt, мога да потвърдя, че са данни от система на ****, но повече информация за това може да предоставят служители на фирма „****“, която поддържа IT инфраструктурата на ****.

ВЪПРОС: Известна ли ви е фирмата Тад Груп ЕООД и свързвала ли се е с вас по-някакъв повод?

ОТГОВОР: Не, не ми е известна тази фирма и не се е свързвала с дружеството ****. Името на фирма „Тад Груп“ ЕООД ми стана известна от медиите във връзка със скандала с изтекли данни от НАП.

ВЪПРОС: Вие предоставяли ли сте тази информация, съдържаща се във файл „****.txt“ на фирма „Тад Груп“ ЕООД или някой от нейните служители?

ОТГОВОР: Не. Заявявам, че ние не сме предоставяли гореописаната информация на „Тад Груп“ ЕООД в този формат. Нямаме сключен договор с „Тад Груп“ ЕООД по отношение на извършване на одит на IT инфраструктурата на ****. Не познавам собственика на „Тад Груп“ ЕООД или техни служители и същите не са влизали в контакт с мен, като изпълнителен директор на **** и физическо лице.

Протокола прочетох лично и удостоверявам с подписа си, че показанията ми са записани правилно.

Разпит на свидетел С. С.

По случая ще кажа следното:

И. Г. който е съсобственик и управител на дружеството **** го познавам от 2005 или 2006г., в приятелски отношения сме. Фирма **** развива туристическа дейност, може би през 2011г. Г. ме помоли да осъвременим и подменим съществуващия сайт с нов на фирмата му – домейна е ****, аз се съгласих. Направих изцяло нов сайт, който е изграден с програмния език „PHP“, като базата данни на въпросния сайт е mysql. Сайтът се хоства на сървъри на дружество ****. Сайтът представлява продуктов каталог. Поддръжката на сайта **** се изразява в актуализиране на информацията която е визуализирана на сайта и създаване на нови функционалности, ако е необходимо. През сайта не се обработва и не се съхранява никаква лична информация дори IP адреси.

От предявената ми експертна справка №**** на стр.12, разпознавам домейна на фирмата ****, в съдържанието на текстовия файл target.txt, може би е изкопирана част от базата данни **** - това е базата данни на сайта ****. От предоставената експертна справка се вижда структура на таблица „locations“, която съхранява част от навигационното меню на сайта ни ****. Аз не съм предоставял горните данни на Тад Груп ООД или на което и да е друго физическо или юридическо лице.

Фирма Тад груп ООД ми е позната от медиите,нямаме сключен договор с тази фирма нито аз нито фирма ****, не съм имал отношения с тази фирма по никакъв повод. Лицата Кристиян Бойков, Георги Янков и Иван Тодоров не ги познавам. Не ми е известно **** да са я наемали за някакви услуги и не са били търсени от въпросната фирма с което да предлагат определени услуги. Не сме правили допълнителни проверки и тестове, всичко си работи нормално.

Протокола прочетох лично и удостоверявам с подписа си, че показанията ми са записани правилно.