Протокол
№

гр. София, 04.06.2024 г.

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 50 състав,**
в публично заседание на 04.06.2024 г. в следния състав:
СЪДИЯ: Мария Бойкинова

при участието на секретаря Ива Лещарова, като разгледа дело номер **919** по описа за **2024** година докладвано от съдията, и за да се произнесе взе предвид следното:

След спазване разпоредбата на чл. 142, ал. 1 от ГПК във връзка с чл. 144 от АПК, на именното повикване в 14:17 часа се явиха:

ЖАЛБОПОДАТЕЛЯТ „АЙ ЕНД ДЖИ ИНШУРЪНС БРОКЕРС“ ЕООД – редовно уведомен за днешното съдебно заседание, представлява се от адв. Г., с пълномощно по делото.
ОТВЕТНИКЪТ Комисия за защита на личните данни (КЗЛД) – редовно уведомен за днешното съдебно заседание, представлява се от юрк. К., с пълномощно по делото.
СГП – редовно уведомена за днешното съдебно заседание, не се представлява.
ВЕЩОТО ЛИЦЕ Н. Н. Х. – редовно уведомен за днешното съдебно заседание, явява се.

СТРАНИТЕ /поотделно/: Да се даде ход на делото.

СЪДЪТ счита, че не са налице процесуални пречки за даване ход на делото в днешното съдебно заседание, поради което

О П Р Е Д Е Л И:
ДАВА ХОД НА ДЕЛОТО

ДОКЛАДВА постъпила молба на 16.04.2024 г. от процесуалния представител на жалбоподателя с формулирани въпроси към назначената съдебно-компютърна експертиза (СКЕ). Приложено е и платежно нареждане относно указания от съда депозит за вещо лице. Молбата е изпратена за становище на ответната страна и в указания срок същата е взела такова.

ДОКЛАДВА постъпила молба по електронен път на 26.04.2024 г. от процесуалния представител на ответника, с която изразява становище относно депозираната на 16.04.2024 г. молба от процесуалния представител на жалбоподателя, като поставя също задачи към вещото лице и представя писмени доказателства, както и пълномощно за процесуално представителство.
ДОКЛАДВА постъпила молба на 30.04.2024 г. от процесуалния представител на ответника със същото съдържание като тази от 26.04.2024 г.

АДВ. Г.: Запозната съм с писмените доказателства, представени от ответника с молбите от 26.04.2024 г. и 30.04.2024 г. Да се приемат.

По доказателствата и доказателствените искания, СЪДЪТ

О П Р Е Д Е Л И:

ПРИЕМА представените с молбата на ответника от 26.04.2024 г. писмени доказателства, а именно: Писмо до КЗЛД с вх. № ПАИКД-13-33#12/02.11.2023 г. и Писмо до КЗЛД с вх. № ПАИКД-13-33#2/05.09.2023 г.

СЪДЪТ ДОКЛАДВА постъпило заключение на 28.05.2024 г. на вещото лице Н. Н. Х. по допуснатата СКЕ, депозирано извън срока по чл. 199 от ГПК, във връзка с чл. 144 от АПК.

СТРАНИТЕ /поотделно/: Да се пристъпи към изслушване на заключението на вещото лице в днешното съдебно заседание по изготвената експертиза, като не възразяваме за срока.

СЪДЪТ ПРИСТЪПИ към изслушване на заключението на вещото лице.
СНЕМА самоличността на вещото лице, както следва:
Н. Н. Х. – 44 г., неосъждан, без дела и родства със страните.
ПРЕДУПРЕДЕН за наказателната отговорност, която носи по реда на чл. 291 от НК. Вещото лице обеща да даде вярно и безпристрастно заключение.
ВЕЩОТО ЛИЦЕ (ВЛ): Представил съм заключение, което поддържам.
АДВ. Г.: Нямам въпроси. Намирам експертизата за достатъчно пълна и ясна, напълно обоснована и правилна.
ЮРК. К.: По отношение на констатациите във въпрос № 4 от експертизата отбелязват, че се касае въвеждане на двуфакторна автентикация от страна на жалбоподателя. Важно е да се отбележи, че всъщност тази двуфакторна автентикация е към момента, когато е изготвена експертизата, а не към момента когато комисията е разглеждала уведомлението и това е констатирано, нали така?
ВЛ: Това е констатация, която е към момента на изготвяне на експертизата. Към онзи предходен момент не мога да кажа, но мога да кажа дали тогава се е случвало някакво нападение, злоупотреба, външно влизане от някой. В смисъл хакерска атака.
ЮРК. К.: И тоест не може да бъде установено дали към момента, когато се е случил неоторизирания достъп до системата Webbroker, жалбоподателят е бил въвел двуфакторна автентикация, така ли?
ВЛ: Не съм имал на разположение система, която е била към онзи момент за

изследване. Към момента каквото е, това мога да установя. Към онзи момент каква е била системата не мога да кажа, тоест достъп или не.
ЮРК. К.: По отношение на въпрос № 8, тъй като възникна противоречие по отношение на констатациите в експертизата и по отношение на информацията, която жалбоподателят е представил пред комисията към момента на разглеждане на уведомлението. От страна на комисията е поискано доказателство за изтриване на стария сървър Линукс, във връзка с което жалбоподателят е представил протокол за изтриване и форматиране от дата 15.06.2022 г. и уведомление от управителя. В отговора, който е формулиран в експертизата се казва, че съгласно установените данни, жалбоподателят е приложил потвърждение за изтрит сървър във фигура № 4 от доклада. Това е фигура, която представя снимка на файла, който хакерът е изпратил като доказателство е видно показване на изтеглен html файл в offline режим, който е отворен през Линукс дистрибуция. В делото не са налице данни, че жалбоподателят сочи и твърди, че е извършен пробив в старите му Линукс сървъри, използвани преди процесния период. Линкът в адресната лента на посочената екранна снимка показва, че не е достъпена базата данни на брокера. Това заключение изпада в противоречие с информацията, която е представена пред КЗЛД в хода на проверката, затова моля вещото лице да обясни.
ВЛ: Реално цялата система не е била на Линукс сървър. Тя не е работила върху такава операционна система. Тя е била на оперативна система Microsoft. Този Линукс сървър е бил в тестов режим и те са се опитвали да го въвеждат в системата, но не е бил въвеждан реално този сървър. Той е бил тестов, а за да се има достъп до тези данни, не е бил изобщо обект на работа. Реално на въвеждане на системата. Той е бил просто за тест и те не са го довършили и не е бил изработен. Те са работили винаги на операционна система Microsoft. Вече там не знам каква е неточността.
ЮРК. К.: Да, но наистина тогава аз трябва да отбележа, че към документацията, която е представена от жалбоподателя в хода на разглеждане на уведомление, не е споменато, че това е тестова среда и във връзка с това възниква противоречие от описаното твърдение на администратора в доклада, че качените от третата страна екранни снимки са направени чрез заснемане на работна станция, а в експертизата е посочено, че същите снимки са направени през изтеглен html файл в offline режим, който е отворен през Линукс дистрибуция, за който същият се твърди, че е изтрит. Това може да се приеме като един вид подвеждане на комисията, защото при постановяването на решението са анализирани абсолютно всички доказателства, които са изискани от администратора.
АДВ. Г.: Може би е добре ВЛ да обясни какво означава отворен през Линукс дистрибуция, за да се внесе техническа яснота. Що се отнася до въобще случая с Линукс, действително с оглед абсолютна пълнота и прозрачност, клиентът е разгледал всички възможности, докато е уточнявал как се е случил инцидентът и затова е решил като крайна мярка да прегледа все пак и изтритата Линукс среда, която се е използвала. За мен няма никакво значение дали жалбоподателя е споменал, че става дума за тестова или извън тестова среда. Факт е, че я е прегледал, установил е че на нея ѝ няма нищо. След допълнителни въпроси на комисията е дал доказателства, че на тази среда не се пази нищо, всичко е изтрито. Така, че за мен въпросът реално е абсолютно неотносим, затова моля ВЛ да обясни какво означава отворен през Линукс дистрибуция.
ВЛ: Говорим за offline, а това означава, че не е в мрежата. Това е файл, който се

отваря върху операционна система Линукс. Това означава дистрибуция. Работата, която е демонстрирана, е изцяло върху операционна система Линукс. Не говорим изобщо за Линукс в настоящата система.
АДВ. Г.: Тоест и хакерът е отворил екранната снимка през Линукс, така ли?
ВЛ: Да, отворена е през Линукс. Това е нов файл, който е изтеглен, Той не представлява някаква официална информация е отворен през операционна система Линукс и е направена екранна снимка.
АДВ. Г.: Самият хакер я е отворил през оперативна система Линукс, а не че е достигнал оперативна система Линукс на нашия клиент, нали така?
ВЛ: Просто снимката, която е направена е на операционна система Линукс. Отворен е един файл, който е offline, означава, че е наличен не през мрежа, отварян в момента на хакване или на някаква такава злонамерена атака. Просто е отворен един файл в конзолна среда, която казва какво е състоянието, не съдържанието и е направена една снимка и така е пратена.
ЮРК. К.: Искам пак да отбележа, че това се констатира постфактум, а не към момента на разследване на инцидента. Полицията многократно е изисквала доказателства, информация която е можело да бъде по-подробно и по-ясно разписана от администратора. За тестова среда, например, никъде не е споменато.
Въпрос на съда към ВЛ: Какво означава суперпотребителски акаунт – този, който е на администратора-разработчик на Webbroker ли?
ВЛ: Нивата на администрация са няколко. „Mastercode“ е най-високото ниво, след това е „Testadm“ – това е администратора, който има достъп графично. Те всичките имат ниво на достъп до едни сървъри, които съответно от своя страна се свързват с базата данни. За да се свали базата данни, трябва да има физически достъп и съответна парола, като физически трябва да е на мястото на компютъра, за да се свали базата данни. Те имат достъп от гледна точка на разработка на сайта – било визуално, било допълнителни кодове, които се програмират с цел да се увеличат възможностите на системата или да се коригират разни дефекти, ъпдейти съответно. А супер-потребителите, това са потребители, които работят със системата – брокери, работни акаунти.
Въпрос на съда към ВЛ: А нерегламентираният достъп казвате, че е със достъп на супер-потребител ли?
АДВ. Г.: Точно така. Това е спорено и с Комисията, защото същата смята, че през достъпа на разработчика се е случвало нещо, а това категорично не е вярно. Още веднъж бих искала да уточня относно Линукс, че мисля, че абсолютно достатъчно доказателства са предадени и към момента на въпросите, които КЗЛД е задавала след уведомлението, тъй като сме доказали, че действително още 2022 г. абсолютно всичко е изтрито на тази операционна система, независимо дали е тестова или не. На нея няма никаква база данни още от 2022 г., така че за мен няма спор в това отношение.
ЮРК. К.: Бих искала да допълня като яснота за съда, че по отношение на спора пробивът е извършен през 2023 г. и за мен не става ясно, след като е изтрито през 2022 г., тоест това не съществува в пространството, как би могло да бъде заснето!?
ВЛ: Предполагам, че това компютърът и системата Линукс е на хакера, който е боравил и си е направил снимки на екрана. Имал е локален достъп на Линукс базирана система, не е отдалечен.
Въпрос на съда към ВЛ: Защото това е една от версиите и Вие казвате, че според Вас представените от хакера снимки са на стария Линукс сървър, нали така?

ВЛ: Този Линукс не е имал права да борави изобщо с базата данни и не е бил в структурата на системата. Той е бил отстрани, тестов, с идеята да се направи огледална система. Това е било Линукс система, която е трябвало да се изгради огледално на функциониращата в момента и в един момент на тестване, по тяхна преценка, да се прехвърли информацията в нейното базиране, да се мигрират данните, но не се е случило.
Въпрос на съда към ВЛ: Как стигнахте до извода, че хакерът е използвал Линукс система?
ВЛ: От снимките реално се стига до този извод. То се вижда.
ЮРК. К.: Дори и с тези изводи и ясни констатации на ВЛ по отношение на случилото се и на системите на администратора, също може да се потвърди извода на Комисията, че администраторът към момента на пробива на сигурността, не е въвел ясни механизми, които да констатират какво се е случило и как да бъде установено. В крайна сметка те не са знаели, че системата им е достъпена, а са разбрали, след като хакерът им е изпратил имейл, което означава, че самата система наистина не е работила добре и това са някакви хипотетични предположения на администратора, които остават недоказани.
ВЛ: Твърдя, че в случая е използван потребителски акаунт, който е заснел тези данни. Системата няма как да отрази, при положение че е направен достъп от потребителския акаунт, който е заснемал данните. Тоест тя не е отразила нищо неестествено, поради което не се е задействала защитата. Същата би следвало да бъде от външни трети лица.
ЮРК. К.: Тук много допринася двуфакторната автентикация, която не е била въведена към момента и която е позволила да се достъпи акаунта.
Въпрос на съда: Какво е двуфакторна автентикация?
АДВ. Г.: Към миналия период също има двуфакторна идентификация. Не разбирам и не мога да взема отношение със сигурност, но в крайна сметка основният начин за манипулиране на действия от външни лица, това са именно „логовете“ и това бе потвърдено и от ВЛ в експертизата. Тоест „логовете“ не показват абсолютно никакъв пробив вътре в системата. Става въпрос за снимки.
ВЛ: Обикновената защита е потребителско име и парола, чрез които се влиза. Двуфакторната е в момента на влизане от системата да се изпрати код на друго устройство, обикновено е телефон, който е въведен вътре в системата. Това е потвърждаващ код. Банките му казват мобилен тоукън (mtoken). Този код се въвежда като бива поискан след вярно въвеждане на потребителското име и парола. Въвежда се и това е достатъчно потвърждение на системата, че това е потребителят. Верифицира го и си достъпва съответния акаунт.
Въпрос на съда към ВЛ: Тази защита имало ли я е в случая?
ВЛ: Към онзи момент не мога да кажа.
Въпрос на съда към ВЛ: Ако допълнително Ви се постави такава задача, ще можете ли да отговорите?
ВЛ: Зависи. Трябва да проверя дали някъде е съобразявано това нещо.
ЮРК. К.: Комисията го е изискала като информация. Има го и приложено като доказателства към административната преписка. Това е отразено и в самото решение.
АДВ. Г.: Може ли, в такъв случай, ВЛ да отговори на въпроса, дали независимо от съществуването или несъществуването на двуфакторна идентификация реално при наличието на достатъчно други технически и организационни методи, които самото

ВЛ завари на място при своята проверка, двуфакторната идентификация въобще от толкова съществено значение ли е, след като действително е доказано, че няма пробив и злонамерени действия?
ВЛ: „Логовете“, които съм анализирал, не показват опити да се извлече информация за акаунтите, многократни опити например с този акаунт да се нацелва паролата, да се прави внедряване на въведен код – всякакви методи, които са познати общо на хакерите, за да се изтегли информация за потребителя, като тази информация да се използва за влизане в акаунта му. Това нещо не се е случило.
ЮРК. К.: Това е въпрос на късмет, че не се е случил някакъв по-дълбок пробив, както е констатирало ВЛ. Тази двуфакторна идентификация дава сигурна сигнализация на администратора, че има външни опити за намеса.
АДВ. Г.: Те не са външни и в случа има огромно значение, тъй като има „n” на брой технически и организационни мерки, които са въведени и които отговарят на целите на системата, а тази система е напълно затворена, тя се използва единствено и само с въпросните достъпи и от брокерите. Тя, както е отговорено и на нашите въпроси, реално няма почти никаква възможност, което може да се потвърди и от ВЛ, за външно влизане през нея. Тоест наличието или не на двуфакторна идентификация по никакъв начин не се отразява на останалите взети мерки и на факта, че тук говорим действително за снимки от очевидно вероятно вътрешно лице, които в крайна сметка аз мога да направя на с телефона си на екран. Това не може да се уточни нито с наличие на двуфакторна идентификация, нито с нейната липса.
Въпрос на съда към ВЛ: На въпрос № 5 Вие отговаряте, че в допълнение към докладите на Webbroker, казвате че използването на „облачна“ среда за съхранение и работа на системата, гарантира на по-високо ниво надеждността. Това към настоящия момент ли е?
ВЛ: Да.
АДВ. Г.: Тя и преди си е била на „облачна“ среда.
ЮРК. К.: Това не може да се докаже, тъй като липсват „лог“-файлове.
ВЛ: Става въпрос за допълнителен въпрос, който не е изследван. Говорим за двуфакторната идентификация.
ЮРК. К.: За „облачната среда“ говорим.
Въпрос на съда към ВЛ: По въпрос № 5, защото Вашето заключение е, че системата е с високо ниво на сигурност, нали така?
ВЛ: Да, с високо ниво е към настоящия момент. Съдейки по докладите, които са правени към онзи момент, една от фирмите, която тя е представила „облачната“ услуга, тя е правила анализ.
АДВ. Г.: Точно така. Това си е още отпреди.
ВЛ: Реално те имат в политиката им за сигурност да съхраняват данните на клиентите. Те имат допълнителни защитни системи освен тези, които се поставят на ползвател.
Въпрос на съда към ВЛ: По въпрос № 9 моля да разясните установено ли е наличие на голям обем трафик на 08.07.2023 г., за което от страна на дружеството не е установена причина?
ВЛ: Не съм установил нещо, което е с пикови стойности и рязко натоварване от конкретен админ. Видно от графиките, това са системни натоварвания, които системата си ги прави сама, когато изпадне в режим на по-ниско натоварване. Това са заложени вътре критерии. Тя използва ресурсите си, за

да си обнови софтуера, да направи проверки за такъв дали е наличен. Това са пиковете, които са извършени, защото те са симетрични. Не е нещо, което да се вижда, че е конкретно заложено или конкретно адресирано към базата данни или към някаква ресурсна система, което няма и връзка с нерегламентирания достъп.
Въпрос на съда към ВЛ: Тоест няма никаква връзка?
ВЛ: Не, това са заявки изходящи, съответно отговор входящ – не е нещо, което да се случи при иницииране на някаква атака или на някакво влизане и желание да се черпи ресурс някакъв.
АДВ. Г.: Да се приеме заключението на ВЛ по допуснатата СКЕ.
ЮРК. К.: Нямам повече въпроси, но си направих много изводи по отношение на експертизата.

СЪДЪТ

О П Р Е Д Е Л И:

ПРИЕМА заключението на вещото лице Н. Н. Х. по допуснатата експертиза.
На вещото лице да се изплати възнаграждение в размер на сумата от 1 200,00 лв., за което се издаде РКО.

Въпрос на съда към процесуалния представител на ответника: Преписката в цялост ли е представена по делото?
ЮРК. К.: Всичко е описано да, дори е номерирано по страници с придружителното писмо. Преписката е окомплектована в цялост.
СТРАНИТЕ /поотделно/: Няма да сочим нови доказателства и нямаме други доказателствени искания.

СЪДЪТ, с оглед процесуалното поведение на страните и липсата на доказателствени искания, счете делото за изяснено от фактическа страна, поради което

О П Р Е Д Е Л И:
ДАВА ХОД НА УСТНИТЕ СЪСТЕЗАНИЯ

АДВ. Г.: Моля да уважите жалбата на представляваното от мен дружество, като отмените изцяло решението на КЗЛД както в частта с предписанията, така и инстанционната част на решението като незаконосъобразно по подробни съображения, изложени в жалбата и в писмени бележки, които днес ще предоставя, с които коментираме и писмените бележки на КЗЛД от февруари месец, както и експертизата, с препис за другата страна. Също така претендирам и разноски, за които представям списък и доказателства за извършването им заедно с писмените бележки.
ЮРК. К.: Моля да отхвърлите жалбата от „АЙ ЕНД ДЖИ ИНШУРЪНС БРОКЕРС“ ЕООД срещу решението на КЗЛД. Решението е законосъобразно, постановено при спазване на материалния закон и административнопроизводствените правила. Комисията в хода на разглеждане на уведомлението от страна на „АЙ ЕНД ДЖИ ИНШУРЪНС БРОКЕРС“ ЕООД е изследвала подробно въведените технически и

организационни мерки от администратора преди констатирания пробив в сигурността и на базата на анализа, който е извършен от страна на комисията, е констатирано, че проведените мерки са недостатъчни, несъобразени с нормите за защита на личните данни, което на практика е довело до констатиране на инцидента, въпреки че, така или иначе, администраторът не е успял да докаже и да установи категорично извличане на данни в своята система. Пробивът в сигурността е факт. Може да бъде прието дори, че снимките са направени от „добронамерен“ хакер, който е констатирал тези пропуски. Администраторът сам не е успял това да констатира. Това е факт, който е доказан безспорно, така че смятам, че Комисията е извършила обективен анализ, във връзка с който е постановено решението. Претендирам юрисконсултско възнаграждение. Представям писмени бележки, които моля да приемете.

СЪДЪТ ОБЯВИ, ЧЕ ЩЕ СЕ ПРОИЗНЕСЕ С РЕШЕНИЕ В СРОК!

Протоколът е изготвен в съдебно заседание, което приключи в 14:51 часа.

СЪДИЯ:

СЕКРЕТАР: