Протокол
№

гр. София, 17.02.2026 г.

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 15 състав,** в публично заседание на 17.02.2026 г. в следния състав:

СЪДИЯ: Росица Цветкова

при участието на секретаря Антонина Митева, като разгледа дело номер **10788** по описа за **2025** година докладвано от съдията, и за да се произнесе взе предвид следното:

На именното повикване в 14,20 ч. се явиха:

ЖАЛБОПОДАТЕЛЯТ – СПЕЦИАЛИЗИРАНА ОЧНА БОЛНИЦА ЗА АКТИВНО ЛЕЧЕНИЕ ВИЖЪН ЕООД – редовно уведомен, не се явява, представлява се от адв. М., с пълномощно по делото.

ОТВЕТНИКЪТ – КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ – редовно уведомен, представлява се от юрк. М., с пълномощно по делото.

ВЕЩОТО ЛИЦЕ – Д. С. – редовно уведомена, не се явява.

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

ОПРЕДЕЛИ:

ДАВА ХОД НА ДЕЛОТО И ГО ДОКЛАДВА.

Делото е отложено за събиране на доказателства, а именно за изслушване на експертно заключение представено на 10.02.2026 г., което не е в срок.

СТРАНИТЕ /поотделно/: Не възразяваме по изслушването на експертизата в днешно съдебно заседание.
АДВ.М.: Вещото лице се свърза с мен и ме уведоми, че пътува към [населено място] и може да се яви в съда след около 40 мин.

СЪДЪТ намира, че предвид изложеното от процесуалния представител на жалбоподателя, делото следва да бъде отложено за по-късен час, поради което

ОПРЕДЕЛИ:

ОТЛАГА производството по делото за 17.02.2026 г. от 14:20 ч. със съгласието на двете страни.

Съдебното заседание продължи в същия състав, секретар и страни в 14:20 часа.
В залата се явява вещото лице Д. С..

СЪДЪТ ДОКЛАДВА Съдебно-медицинска експертиза депозирана на 10.02.2025 г. и изготвена от вещото лице Д. С..
СЪДЪТ ПРИСТЪПВА КЪМ ИЗСЛУШВАНЕ НА ЗАКЛЮЧЕНИЕТО НА СЪДЕБНО-КОМПЮТЪРНАТА ЕКСПЕРТИЗА, при съгласие на двете страни, изразено изрично.
СНЕМА САМОЛИЧНОСТТА НА ВЕЩОТО ЛИЦЕ, КАКТО СЛЕДВА:
Д. С. – 48-годишна, българка, българска гражданка, без дела и родство със страните.
СЪДЪТ предупреди вещото лице за наказателната отговорност, която носи съгласно чл. 291 НК.
ВЕЩОТО ЛИЦЕ С.: О. да дам вярно и добросъвестно заключение. Поддържам заключението.
Относно посоченото на стр. 16 за реакцията на служителите по осуетяване на екстрадирането на данни в рамките на един час, според всички добри световни практики реакцията е много повече от задоволителна при решаването на такъв проблем.
Пробивът е в 3 часа. Администраторските права, с които той е достъпил машината са в 5 часа и 19 минути, тоест той тогава получава пълен достъп. Той получава пълен достъп до всички машини, чак в 5 часа и 19. Той в 3 часа влиза в мрежата, но докато се ориентира и докато създаде необходимата инфраструктура, за да може да прави неща минават някъде около 2 часа. В 5 часа и 19 минути той е успял администраторски да достъпи машините на сървърите. Един час е от момента, в който е настъпил достъпа на нерегламентирания потребител до момента, в който му е спрян достъпът, това е един час, иначе са три часа, но три часа също е време в което, според

световните практики, се смята за доста добра реакция.

Тъй като нямаше как да се изследват машините, които са работили вън фон са запазени снимки от телефони, така наречените „скрийншоти“ (screenshot) или снимки на екран на сървърите, които служителите са заснели по време на този инцидент. И всъщност една част от анализа е направена по тези снимки хронологично, за да могат да се обяснят и навържат нещата.

Имат инсталирано и сега и в момента на атаката са имали нещо като аларма. Системните администратори са направили аларма да получават имейл, когато някой влезе от съмнителен Ай Пи адрес (IP adress) по имейл. Между другото, имейлът си стои и до настоящия момент и е анализиран, защото той е на мейл-сървър, който е съвсем отдалечен.

Системата така са си я настроили, че да може при нерегламентиран достъп вътрешен потребител да изпраща съобщение до двамата системни администратори. Вътрешен потребител е този рутер вижънклиник (visionclinic.bg). Вътрешен потребител означава, че това е домейна (domain) на клиниката.

Всички служители имат имейл в този домейн. От този домейн е направен имейл-акаунт рутер (email account – „router“), който служи за изпращане на такъв тип аларма. Всички служители имат имейл в този домейн. В случая системните администратори са си дали и лични имейли от съображение за сигурност да не могат да се достъпят в служебната поща и поради тази причина е изпратен на имейл на А. в джимейл (Gmail).

Линкът, когато се направят определени действия, служи на този, който го е изпратил, да получи някакъв достъп до машината на този, който е натиснал линка. Този, който натиска линка няма администраторски права дори до своята машина. От там нататък, този, който влиза, започва да търси други канали, за да се сдобие с администраторски права на всички машини. Л. изпратен по имейл и натиснат от служител по никакъв начин не активира такъв вирус, който да започне да точи данни. Той служи единствено за вход и начин за сдобиване с администраторски права до машините и сървърите. След като се сдобие с администраторски права, тогава вече може да криптира и да извлича. Системата обхожда на около 15 минути и не може непрекъснато в реално време.

Има данни, че в 3 часа започва, но преди три часа няма данни. Няма данни в рутера за Ай Пи адреси (IP-адреси), които са достъпвали мрежата и които никога до сега не са я достъпвали. В 3 часа е първия част, в който е достъпена тази система. В 3 часа и 17 минути се получава тази аларма.

Има запазени данни от мейл сървъра и запазени данни от рутера. От нищо друго няма запазени данни. И както казах, тези снимки, които са направени от системата администратори са в момента на тази атака. Данните ги взимат логовете от рутера (router log in) и от мейл сръвъра (mail server). Данните от мейл сървъра (mail server) могат да бъдат приложени, но аз не виждам някаква причина. Това е просто начин, по който служителите да бъдат уведомени, ако нещо се случва с тяхната система. Л. файловете от 08 февруари не се пазят. Алармата от рутера е еднозначен показател, че хакерът е влязъл в 3 часа. Това са обективни данни, а не са само по сведение на служителите. Алармата създадена като такъв тип имейл сигнализира не само за хакерски атаки, а и за други неща, които са необичайни за поведението на тази система. Когато служител получи такъв имейл, той си прави проверка, какво точно се случва в системата. В някакъв момент вече те нямат права отдалечено, защото този, който е влязъл е получил вече пълен достъп и им е отрязал всякакви права и тогава вече отиват на място и дърпат шалтера.

Сървърите са малко повече в настоящия момент и малко по-добре защитени с двуфакторна верификация (two factor authentication) вече. Но протокол при изследване на такъв вид атаки, при положение, че няма, най-чисто е да се вземе в машината и да се изследва какво точно се е случило. Нали взимам я в моята лаборатория, закачам я и започвам да изследвам какво точно се е случило, но в случая това нямаше как да се случи. Прибягва се до следващите точки в протокола - започва да се обследва този вирус, защото тези сървъри са вече форматирани и се използват отново, те не са си купили нови. Това не е техника, която може да си купи човек всеки ден.

Следващия начин съм обяснила в експертизата – 3 подхода са използвани, какво точно се случва при нападение от този вирус в други системи по света. Изследвано е от специалист, има данни, има изводи направени и на базата на това, което аз изследвах, прочетох и видях точно за този вирус направих и тези изводи в експертизата. Във връзка с тези скрийншоти, които съм разгледала, те времево съвпадат с начина, по който е описан този вирус в литературата.

Логове бяха запазени до дата 02.02., което е 6 дни преди атаката. Тези логове бяха прегледани и по тях е установено как е работила системата преди тази атака. Логове има и след атаката и по тях се прави равносметка какво се е променило след това. Така че това е начинът по който се установи как е била създадена тази система преди и след. Има данни, но в тези логове няма подробна информация какво точно се е случило по време на тази атака, как точно са направени връзките между системите. Няма чак толкова подробна информация. Има информация, която се взима предвид, но не е такава информация, чрез която аз да кажа в колко часа някой е влязъл,

изтеглил е такива данни и е излязъл.

Обективни данни за мерките преди това се взимат на базата на логовете до 02.02.

Двуфакторната верификация (two factor authentication) стана широко използван метод за защита през 2025 година. До 2024 година не беше толкова популярна. Въпросът не е дали някой някога ще пострада, въпросът е кога това ще се случи, без значение колко много препятствия се слагат в една система, тя в някакъв момент е уязвима. Логове от сървъри и логове от рутер са били запазени. Няма ги преди инцидента, за последно са от 02.02. и се дължи на това, че тези логове се запазват на определено време, или просто не са успели да възстановят тези логове когато са възстановявали системата, тоест логовете също са били криптирани. Дали криптирани или изтрити няма особено голяма разлика в крайния резултат, защото криптираните също не могат да се разчетат.

АДВ. М.: Моля да приемете експертизата като обективна пълна и всестранна. Представям и моля да приемете следните документи : Заповед № РД-6 от 08.02.2021 г, Заповед № РД-9 от 22.03.2021 г., Заповед № РД-4 от 20.03.2023 г., Заповед № РД-5 от 26.04.2023 г., издадени от управителя на СОБАЛ „Вижън“ ЕООД; Уведомление от СОБАЛ „В.“ до Министерство на вътрешните работи с изх. № 22 от 09.02.2024 г.; Уведомление от СОБАЛ „Вижън“ до Министерство на здравеопазването и „Информационно обслужване“ АД с изх. № 23 от 09.02.2024 г.; Уведомление от СОБАЛ „Вижън“ до Министерство на здравеопазването: и „Информационно обслужване“ АД с изх. № 25 от 15.02.2024 г.

ЮРК. М.: Не възразявам по експертизата. Моля да се приеме. Представям писмено становище по отношение на експертизата. Тя в своята цялост представлява един експертен анализ на предоставени документи от администратора. Тъй като са минали повече от две години от извършване на нерегламентирания достъп до системите и както и вещото лице е записало в своята експертиза, че засегнатите сървъри са форматирани, преинсталирани и се пазят частично логове и данни, така че не мисля, че казва кой знае какво за момента на пробива.

Не възразявам по приемането на представените документи от жалбоподателя.

СЪДЪТ по доказателствата

ОПРЕДЕЛИ:

ПРИЕМА и ПРИЛАГА заключението по съдебно-компютърната експертиза от 10.02.2025 г., изготвено от вещото лице Д. С.

ОПРЕДЕЛЯ окончателно възнаграждение за вещото лице в размер на 1578 (хиляда петстотин седемдесет и осем) евро, от което да се изплати стойността на внесения депозит 255,65 (двеста петдесет и пет и 0,65) евро, а за разликата следва да се задължи жалбоподателя.
ЗАДЪЛЖАВА жалбоподателя да внесе по депозитната сметка на съда сумата от 1322,35 (хиляда триста двадесет и две и 0,35) евро в 7-дневен срок от днес.
УКАЗВА че при неизпълнение в срок съдът ще предприеме действия по принудителното събиране на сумата.
Да се издаде на вещото лице РКО за остатъка след представяне на доказателства за внасяне на сумата.
ПРИЕМА и ПРИЛАГА представените в днешното съдебно заседание документи от процесуалния представител на жалбоподателя и писменото становище от ответника.

СЪДЪТ, като счете делото за изяснено от фактическа и правна страна

ОПРЕДЕЛИ:

ДАВА ХОД НА ДЕЛОТО ПО СЪЩЕСТВО.

АДВ. М.: Моля да постановите решение, с което да уважите депозираната жалба по изложените в същата подробни аргументи. Моля да ни присъдите разноските по делото, за което представям списък. Моля за срок за писмена защита.

ЮРК. М.: Моля да постановите решение, с което да отхвърлите жалбата като неоснователна и недоказана и да потвърдите обжалваното решение. Комисията недвусмислено е констатирала, че администраторът е допуснал нарушаване на сигурността на личните данни, които събира, обработва и съхранява при осъществяване на дейността си. Компютърната система на СОБАЛ „Вижън“ ЕООД, включваща три сървъра и електронен архив са засегнати изцяло. Това е предоставил като информация администратора по време на проверката. Като отговор на Въпрос № 6 от писмо 1315#2/26.02.2024 г. на по-късен етап по време на проверката се споменава, че все пак е открит някакъв незасегнат архив на файловия сървър, обаче архивът с каква информация е бил? актуална ли е била? Имало ли е всички лични данни на засегнатите близо 58 000 физически лица? Такава информация не е предоставена. Когато говорим за електронен архив в случай на хакерска атака, то се очаква той да бъде добре изолиран, защитен, за да може след това да бъдат

възстановени данните, които са засегнати. Както казах засегнатите са близо 58 000 физически лица, като някои от тях са лица под 18 годишна възраст към датата на пробива. Категорията лични данни засегнати от нарушението са имена, ЕГН-та, паспортни данни, телефонни номера, имейл адреси, и документация свързана с прегледи и изследвания. Към момента на пробива е имало загуба на способност за предоставяне на критична услуга, тоест отменени са няколко операции, заради които не е могла да се възстанови документацията. Злонамерената атака е довела до тотално унищожение на операционните системи на трите сървъра, като в хода на проверката администраторът е представил оценка на риска извършена през 2019 г., което е 5 години преди инцидента и в настоящото и в настоящото заседание представи преразглеждане през 2021 г. и 2023 г., което с едно изречение, че тя е актуална. Съгласно чл. 32 от общия регламент, администраторът е задължен да извършва периодични оценки на риска, особено когато говорим за чувствителни данни каквито са характерни за болници. Без значение дали са събрани достатъчно доказателства за реалното използване на тези данни от третото лице, достатъчен е факта, че е нарушена сигурността на личните данни, което създава вероятност за осъществяване на което и да е от събитията, посочени в чл. 4, § 12 от Регламент (ЕС) 2016/679. Подробни аргументи излагам в писмени бележки, които представям. Моля за юрисконсултско възнаграждение. Правя възражение за прекомерност на адвокатско възнаграждение.

СЪДЪТ ДАВА ВЪЗМОЖНОСТ на процесуалния представител на жалбоподателя в 7-дневен срок да представи писмени бележки.

СЪДЪТ ОБЯВИ, ЧЕ ЩЕ СЕ ПРОИЗНЕСЕ С РЕШЕНИЕ В ЗАКОНОУСТАНОВЕНИЯ СРОК.

Протоколът е изготвен в съдебно заседание, което приключи в 14,52 часа.

СЪДИЯ:

СЕКРЕТАР: