Протокол
№

гр. София, 09.06.2026 г.

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 50 състав,** в публично заседание на 09.06.2026 г. в следния състав:

СЪДИЯ: Мария Бойкинова

при участието на секретаря Ива Лещарова, като разгледа дело номер **10789** по описа за **2025** 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 13:45 часа се явиха:

ЖАЛБОПОДАТЕЛЯТ „Специализирана очна болница за активно лечение „Акад. Пашев“ ЕООД – редовно уведомен за днешното съдебно заседание, представлява се от адв. М., с пълномощно по делото.
ОТВЕТНИКЪТ Комисия за защита на личните данни (КЗЛД) – редовно уведомен за днешното съдебно заседание, представлява се от старши експерт (СЕ) М., с пълномощно по делото.
ВЕЩОТО ЛИЦЕ Н. Н. Х. – редовно уведомен за днешното съдебно заседание, не се явява.

АДВ. М.: Да се даде ход на делото. Предвид изявлението на вещото лице, че в 13:40 часа има заседание в Софийски градски съд (СГС), за което ме уведоми преди заседанието, моля да го изчакаме и да отложим делото на второ четене, за да можем да изслушаме експертизата в днешния ден.

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 постъпило заключение на вещото лице Н. Н. Х. по допуснатата съдебно-компютърна експертиза (СКЕ), депозирано на 28.05.2026 г. в срока по чл. 199 от ГПК, във връзка с чл. 144 от АПК.

СЪДЪТ намира, че следва да даде възможност на вещото лице Н. Х. да представи изготвеното заключение по допуснатата от съда експертиза в днешното съдебно заседание, след приключване на ангажиментите му в СГС по дело, което е насрочено в 13:40 часа, затова

О П Р Е Д Е Л И:

ДАВА ВЪЗМОЖНОСТ на вещото лице Н. Х. да представи изготвеното заключение по допуснатата от съда експертиза в днешното съдебно заседание, след приключване на ангажиментите му в СГС по дело, което е насрочено в 13:40 часа

СТРАНИТЕ /поотделно/: Не възразяваме. Ще изчакаме вещото лице, след което ще продължим с делото.

След спазване разпоредбата на чл. 142, ал. 1 от ГПК във връзка с чл. 144 от АПК, на именното повикване на второ четене в 14:09 часа се явиха:

ЖАЛБОПОДАТЕЛЯТ „Специализирана очна болница за активно лечение „Акад. Пашев“ ЕООД – редовно уведомен за днешното съдебно заседание, представлява се от адв. М., с пълномощно по делото.
ОТВЕТНИКЪТ Комисия за защита на личните данни (КЗЛД) – редовно уведомен за днешното съдебно заседание, представлява се от старши експерт (СЕ) М., с пълномощно по делото.
ВЕЩОТО ЛИЦЕ Н. Н. Х. – редовно уведомен за днешното съдебно заседание, явява се.

СТРАНИТЕ /поотделно/: Да се пристъпи към изслушване на вещото лице.

СЪДЪТ ПРИСТЪПИ към изслушване на заключението на вещото лице.

СНЕМА самоличността на вещото лице, както следва:
Н. Н. Х. – 46 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: Представил съм заключение в срок, което поддържам.

На въпроси на адв. М. вещото лице отговори:
Представям малко история на цялата атака. Тук става въпрос за две болници – едната е „Вижън“, другата е СОБАЛ „Акад. Пашев“ ЕООД. Те се поддържат да кажем от един системен оператор, като двете системи са свързани през криптиран канал, защитен между тях си. Реално системите можем да кажем, че се помещават в една виртуална среда, на едно физическо място и реално атаката по хронология, която следва, която съм видял е тръгвайки от този имейл. И. се издава от виртуалната среда като защитен механизъм, че има нередност и същият тръгва от клиника Вижън. Реално заразяването тръгва от клиника Вижън и нейната система цялата е третирана и блокирана, но докато стигне до СОБАЛ „Акад. Пашев“ ЕООД, там също успява да навреди, в смисъл да блокира системата, но не е успяла да зарази един вид архивите, които в последствие чрез тях те са възстановили в СОБАЛ „Акад. Пашев“ ЕООД. Действията, които са извършени от системния администратор и които съм описал за двете болници ги приемам не за идентични.
СЕ М.: Н. само да се конкретизира отговора за СОБАЛ „Акад. Пашев“ ЕООД.

На въпроси на адв. М. вещото лице отговори:
Действията са предприети в един и същи момент, защото системата е свързана. Било е въпрос на първоначално заразяване на системите и вече афектирането им от това заразяване. Това е било поетапно вече. Говорим за СОБАЛ „Акад. Пашев“ ЕООД, която е била второстепенна в това заразяване.
АДВ. М.: Във връзка с тази аларма на стр. 3 от заключението, на която казвате, представям и моля да приемете извадка всъщност от още един мейл, който е получен и който е предоставен на вещото лице, с препис за насрещната страна. И тъй като на вещото лице му е осигурен достъп на място в болницата и същото е проверило системите, моля да се приеме като писмено доказателство по делото и да се предяви на вещото лице, за да отговори дали освен тази аларма, която е посочил на стр. 3 от заключението, то този имейл също е видян, проверен и дали се отнася по същия начин и за атаката.
СЕ М.: Възразявам, защото това е текст от имейл, не се вижда от кой до кого е изпратено. Това се вижда, че е препратено писмо.
СЪДЪТ ВРЪЧИ представения документ от процесуалния представител на жалбоподателя на вещото лице (ВЛ) Х..
ВЛ Х.: Реално това се изпраща от алармиращата виртуална среда.
На въпроси на адв. М. вещото лице отговори:
Алармата, за която говоря в заключението, касае точно изключването на системата, че тя спира да функционира, че се криптира. И тъй като така е поставен въпросът, а именно да се проследи реално заразяването, което тръгва от друга клиника. Това е постфактум.
Мерките, които съм анализирал в отговора си на въпрос № 9, тук става въпрос за мрежова и информационна сигурност. Това означава, че системата по начина, по който е виртуализирана и мерките, които са сложени в системата, в която доставя интернет са основополагащи за средно ниво на сигурност, което защитава системата, но не може да изключи по никакъв начин други атаки. Визирам под други атаки злонамерени атаки, които могат да блокират по някакви други методи. Доколкото разбирам този вирус изисква не пробив на тази система по начина, по който е конфигурирана, а изисква внедряването му чрез достъп било локално или мисля, че чрез използването на канала за здравноосигурителната система, който не е криптиран, но пък от друга страна може да влезнат там вируси на други слаби места, които са много по-ниско защитени спрямо цялата сигурност, която е направена за системата. Но тези канали и възможности са извън защитата на тази система.
Относно изявлението ми в заключението на стр. 2, че съм анализирал в действителност над 100 случая с подобен тип пробив, искам да добавя, че с колежка сме правили подобни експертизи и сме изследвали това като отделно заразяване към други мрежи. Известни са няколко такива. „Ransomware“ е известен от много години вид злонамерен софтуер, който е нанесъл щети за милиони. В случая говорим само за този тип пробив, като също са описани такива случаи. Говорим и за други болници. „Ransomware“ е атаката, този зловреден код, който криптира реално и изисква откуп. Говорим за сходен тип вирус със сходен тип криптиране, защото тези вируси се различават по вида, методологията за криптиране. Тоест ключът, който заключва данните е различен при всичките тези еднотипни вируси на действие. В случая тук се използва алгоритъм, който не е известен на крипто лабораториите, които се борят с този проблем. Периодът е горе-долу идентичен, в рамките на няколко месеца. Мисля, че беше на седмици този вид „Backmydata, тоест една и съща дата, масирано.
Говорим за автоматични мерки, които предпазват цялата система от външен тип атака. Тук в случая може да се използва чрез локално, да кажем и флашка, която се поставя без никакво

действие, всички тези мерки отпадат. В смисъл те не са годни да защитят системата и тя бива атакувана по друг начин, като защитата е насочена към предпазване на данните от външни намеси. Например от незнание някой служител може да сложи едно устройство, което да криптира цялата система и цялата ѝ защита. Няма отношение към този вид атаки. Говорим и за антивируси, които не разбират типа на вируса и че това е вирус злонамерена атака и не могат да се защитят. Това е просто новонаписан крипто код, който не бива да бъде хващан от антивируса.
В конкретния случай нямаме данни от къде точно е произтекла атаката, поради причината че този вирус е основополагащ в неговото действие той да нанесе щетите и да прикрие следите от начина си на постъпване в системата.
От логовете установявам каква е била конфигурацията на защитата, каква виртуална система е била ползвана и какви са били настройките на рутера, който е бил необходим за свързването устройството, тоест на системата към интернета. Реално ние ревизираме по-скоро такава защита през интернет. Според мен е по-скоро не като личен характер, а локален, физически, но не мога да го докажа.
На въпроси на СЕ М. вещото лице отговори:
В СОБАЛ „Акад. Пашев“ ЕООД данните са били криптирани, но не са били криптирани в степен цялата система. Останал е архивът на системата от преди седмица. Тогава се е правил към онзи момент на всяка седмица и това е по думи на администратора. Впоследствие са използвали този архив, за да възстановят данните. Данните са криптирани така, както съм посочил в т. 6 на стр. 2 от заключението.
СЕ М.: Правя едно уточнение във връзка с тези писма на клиника „Вижън“ и СОБАЛ „Акад. Пашев“ ЕООД. Вещото лице каза, че първо е заразена системата на клиника „Вижън“, а след това системата на СОБАЛ „Акад. Пашев“ ЕООД. Ако приемем, че това е оригинално съобщение, този час е преди сигнализацията за заразяване на системата на СОБАЛ „Акад. Пашев“ ЕООД. Съобщението на клиника „Вижън“ е в 03:17 часа, а на СОБАЛ „Акад. Пашев“ ЕООД в 03:02 часа.
ВЛ Х.: Това не е релевантно към системата кога отговаря точно, че има някакви проблеми с нея. Аз съдя по последващия факт, заразяване на системата на СОБАЛ „Акад. Пашев“ ЕООД, че там не е успяло да се заключи всичко. А другата система е била тотално компрометирана и не е останало нищо.
СЕ М.: Искам да обърна внимание, че екранната снимка на това съобщение касае препратено писмо от А. Г., предполагам лична негова поща, до А. Г., клиника „Вижън“. Вие видяхте ли, беше ли Ви предоставено оригиналното съобщение?
На въпроси на СЕ М. вещото лице отговори:
Само тези, които са препращани. Реално това е лицето, което отговаря за системата и той реално си е препращал съобщенията, като съм съгласен, че може и самото съобщение да бъде модифицирано. Алармата, която е известила системния администратор се изразява в това, че технологично не можем да разберем в случая какво е било, но е била настроена аларма към онази система, която е била заключена в онзи момент. Аз нямам достъп до тази система, която е компрометирана, тоест до нейните настройки към онзи момент. Не мога да преценя алармата какво известява, в случая какъв етап от проблем с нейното нефункциониране известява. Бяха ми представени логове на системите от преди това, по които съдя как е настроена сървърната система с HYPER-V CLUSTER и логовете от настройките на рутера, тъй като не се пазят логове от дена на инцидента. И това е преди инцидента, но по часове, по дни не мога да кажа с точност. Трябва да погледна. Съдейки от вида на атаката самите логове, те са кодирани, те са недостъпни, нямаме достъп до тях. Целта на този вирус е да заключи така информацията, че да не бъде достъпна, а чрез изпращане на код от някъде, неизвестно от къде, чрез откуп при съответната

сума, която бива заплащана, да се отключат данните. Ние нямаме ключа. Имайки предвид какъв е вирусът е възможно той да бъде ексфилтриран чрез линк, отворен от служител на имейла. Тези вируси реално като тежест, като изпълнение представляват един алгоритъм, който трябва да се изпълни върху компютъра и един вид не са трудни за инсталиране. Лесно се придобива той с линкове и не изисква голям обем, който да бива свален на компютъра, за да се стартира процеса по заключване. Могат да бъдат стартирани с всякакви мерки, тоест с всякаква връзка. Тъй като не са налични други логове, които може да се изследват, по-скоро можем да бъдем сигурни, че точно в този час е осъществен пробивът. Информацията, която се е съдържала в незасегнатия сървър, е архивът. Вътре се съхраняват лични данни. Това е цялата система на болницата, която е работила една седмица по-рано. Архивирала се е седмично, сега вече е почасово всеки ден, като може да се потвърди, че данните вътре са актуални към датата на архивиране, не към датата на криптиране. Говорим за седмица по-назад, а не за точния момент, откогато настъпва криптирането. Не съм изследвал какви лични данни се съдържат вътре, но са на пациентите – всичко, което е необходимо за работа на болницата и на цялата система. Не съм изследвал дали се съдържат болнични листове, но това е цялата система като база данни реално. Все едно всичко, което се случва. Преинсталирането е след това, което се е случило, след криптирането. Към датата на пробива мерките са били единствено по тези логове по съобщенията, които са създадени. Логовете са от рутер, който не се преинсталира. Той бива конфигуриран по друг начин. Логовете към онзи период не се променят и тези имейли, които са основата. Техническите и организационните мерки към деня на пробива се изразяват в това, че в рутера можем да видим само какви са настройките преди пробива и реално той за каква мрежа отговаря. Настройките са на достъпа до интернета. Там е конфигуриран този VPN канал за връзка между болниците. Това може да бъде, като е само за VPN канала, не за останалите технически и организационни мерки. За цялата мрежа и нейната конфигурация вътре не. Това може да видим от самите сървъри и виртуалните машини, но не разполагаме с логовете, които са се случили по време на криптирането, защото те са били унищожени при заключването. Снимката на стр. 4 от заключението показва, че сървърите на двете болници са на едно място към онзи момент. Говорим за една локация. В случая това е видеозаснемане, което е видео от охранителните системи. След това на същата страница е криптирането. Това реално, където проследяваме и по някакъв начин черпим всякаква информация от другата система като датиране. Първата снимка ми е предоставена, както и втората, но на живо не съм виждал тази папка на компютъра. Но съм изследвал мета данните на самите снимки, които нямат модификация. Възможно е и преди да бъде направена снимката нещо да бъде изтрито като папка.

На въпроси на съда вещото лице отговори:
Ексфилтрацията на обем 10 TB в рамките на 1 час е технически невъзможна, тоест това означава, че при конфигурацията и при интернет достъпа, възможността за трафик в рамките на 1 час този обем информация не може да бъде изтеглена през, да кажем, конфигурацията на интернета. Тоест скоростта не позволява да се изтегли такъв обем за 1 час.
Има няколко метода за трансфер на лични данни. Операторът, тоест доставчикът на интернет да не е сканирал данни. Може да се провери от системата, но тя е криптирана. Това се е случило и реално технически много сложно за конфигуриране на една система да е натоварена със самозаключването си с неизвестен код и това да споделя информация със сигурния капацитет. От тази зловредна атака не мога да кажа категорично дали са изтекли лични данни, но на този тип атаки, които изследвам отдавна, не е това целта да се тегли информация, а да се заключи и да са с

код.
СЕ М.: Вещото лице поясни, че той разполага с тези данни и от това писмо, което е индикирало за нещо, което се случва в системите, може да заключи, че тогава е осъществено, но всъщност няма категорични доказателства, че то не е станало по-рано и че реално може хакерът да е разполагал с повече време, а не с 1 час.
ВЛ Х.: Теоретично ако е имал достъп преди да криптира данните, то е могло да свали цялата система. Няма следи. Ако има някакви доказателства, че е имал някакъв пълен достъп до системата, той е могъл да я изтегли и преди това, но говорим за теория. Това е което трябва да се случи седмици назад във времето, за да не бъде хванато от системата. Не мисля дори, че хакер е проникнал в системата е че по някакъв начин е включил този вирус. Каква е идеята, мотивът не мога да разбера реално.
Не е типично за атаки, които целят да повредят дадена система или да вземат някакъв ресурс, било то финансов или да изтеглят информацията, да се правят първо опити за сваляне на информация и след това да се криптира, защото това е чувствителна система, която всъщност се самосъхранява и при един такъв нерегламентиран достъп все някъде ще индикира нещо и при следващия етап от криптиране може да бъде неуспешен. Реално целта на атаките е да бъдат успешни. Говорим за две различни неща – да се тегли информация и да се криптира, което този вирус не прави. Същият не тегли информация.
На въпроси на адв. М. вещото лице отговори:
Реално това, което съм установил е относно това дали говорим за пробив за извличане на данни или за криптиране чрез този зловреден софтуер са две различни неща. Самият вирус може да работи и да заключва информацията по време на действията на администраторите. На снимките на стр. 4 от заключението не се вижда криптиране. То се вижда на стр. 5 от същото, като отгоре се виждат данните, които са криптирани. Може да се криптира, както казах, с една флашка, която сеи поставя в някой локален компютър. Никакви права не са необходими. Вирусът е така устроен, че заразява компютрите и си има администраторските права. Не му е необходим администраторски достъп или дори от компютър с ограничени права пак може да бъде заразен, като целта на заразяването е операционна система W. единствено, която чрез заразяването си дори на локално ниво, при нейната комуникация с по-висшите стоящи сървъри предава такава информация, където споделя и този процес на криптиране и той бива споделян към другите системи и така работи и вирусът, като не са му необходими администраторски права. Това, че нещо е възможно да бъде изтрито не променя факта, че хакерите са получили администраторски права едва след 05:19 часа. Самият вирус, за да осъществи криптирането, той трябва да прочете файла. Има заложена схема в него всеки файл, разширението, какво съдържа и дали е потенциална цел за него. По разширението той разбира целевата му група. След като направи списък, заразяването се изразява в един вид „архивиране“, тоест модифициране на файла, чрез добавяне на парола, който бива кодиран и преди това е ключът. Реално при добавянето на кода и заключването на този файл оригиналът се изтрива и се замества. Имаме изтриване на стария файл, копиране на нов с основната информация с ключа, вече заместен такъв, с основно име и променено разширение, което е вече резултатът от заключването и ако системата бива анализирана за изтекли файлове, ще се видят всички оригинални файлове са изтрити, но невъзможно и да бъдат възстановени. В случая е така. Може да се видят старите файлове, които са изтрити и това го прави автоматичния процес на вируса. Той ги

замества по съдържание върху тях.
СЪДЪТ ДОКЛАДВА справка-декларация, подадена от вещото лице Н. Х., с която заявява, че окончателната сума за изготвяне на заключението е в размер на 944,00 евро, поради което

О П Р Е Д Е Л И:

ПРИЕМА заключението на вещото лице Н. Н. Х. по допуснатата експертиза.
ОПРЕДЕЛЯ окончателен депозит за възнаграждение на вещото лице Н. Х. в размер на 944,00 евро.
На вещото лице да се изплати възнаграждение в размер на сумата от 511,29 евро, за което се издаде РКО.
ЗАДЪЛЖАВА процесуалния представител на жалбоподателя в 7-дневен срок, считано то днес, да заплати разликата в размер на сумата от 432,71 евро евро за изготвяне на експертизата.
След което на вещото лице Н. Х. ще се издаде РКО за довнесената сума.
По доказателствата и доказателствените искания, **СЪДЪТ**

О П Р Е Д Е Л И:
ПРИЕМА представеното доказателство в днешното съдебно заседание от процесуалния представител на жалбоподателя.
СЕ М.: Подготвила съм становище по отношение на експертизата, което представям на съда, с препис за насрещната страна.
СТРАНИТЕ /поотделно/: Нямаме други искания по доказателствата.
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. М.: Моля да постановите решение, с което да уважите изцяло жалбата срещу решението на КЗЛД по подробни аргументи, изложени в същата. Моля да ми предоставите кратък срок за писмена защита, в рамките на която да уточним изводите не вещото лице, включително и в днешно съдебно заседание. Молим да ни присъдите сторените по делото разноски, за което представям списък и доказателства за извършването им, с препис за насрещната страна.
СЕ М.: Оспорвам жалбата. Моля да я отхвърлите като неоснователна и недоказана и да потвърдите обжалваното решение. В хода на разглеждане на уведомлението КЗЛД е констатирала, че администраторът е допуснал нарушение по отношение на личните данни при осъществяване на своята дейност, а именно че трето злонамерено лице е осъществило неправомерен достъп до компютърната система на СОБАЛ „Акад. Пашев“ ЕООД, включваща 3 сървъра. Електронният архив се съхранява на отделен сървър, който също е засегнат от хакерската атака. Това е информация, предоставена от дружеството в писмо рег. № ПАИКД-13-16#2 от 27.02.2024 г., отговор на въпроси 5 и 13. На по-късен етап по време на проверката се споменава, че е отрит някакъв незасегнат архив на файл без сървър, обаче каква информация се съдържа в този архив не е ясно. Не е представена информация от дружеството. Администраторът съобщава, че данните

са били криптирани и базата данни недостъпна, като след възстановяване на работа не може да се определи какъв е точният списък на засегнатите лица. Засегнати от нарушението са над 15 хил. физически лица, някои от които деца на възраст под 18-годишна възраст към датата на пробива. Сред категориите лични данни засегнати от нарушението са физическа идентичност на лицата, социална идентичност и специални категории данни. Злонамерената атака е довела до тотално унищожаване на операционните системи и настройки на три сървъра. В хода на проверката администраторът е представил анализ на риска във връзка с обработването на лични данни на физическите лица, извършено преди нарушението на 07.01.2020 г., което е 4 години преди инцидента. Следва да се отбележи, че по чл. 32 от Регламента администраторът е задължен да извършва периодични оценки на риска, без значение дали са събрани доказателства относно реалното използване от трето лице на процесните лични данни, за което е осъществен нерегламентиран достъп. Достатъчен е фактът на нарушена сдигурност на личните данни, който създава вероятност за осъществяването на което и да е от събитията, посочени в чл. 4, § 12 от Регламента (Регламент (ЕС) 2016/679). Подчертавам, че комисията е надзорен орган, не разследващ орган и е в тежест на администратора на лични данни да докаже, че е приложил подходящи технически и организационни мерки. Подробни аргументи излагам в писмени бележки, с препис за другата страна и с оглед изхода на спора претендирам юрисконсултско възнаграждение.

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

ДАВА ВЪЗМОЖНОСТ на страните да представят писмени бележки по делото в 14-дневен срок, считано от днес.

Протоколът е изготвен в съдебно заседание, което приключи в 14:47 часа.

СЪДИЯ:

СЕКРЕТАР: