

Универзитетска клиника у Диселдорфу нашла се на мети хакера који су хтели новац. Очигледно је читава акција била забуна коју је животом платила једна пацијенткиња. Сада се поставља питање безбедности немачких болница, пише Дојче веле (DW).



Како пише DW, државно тужилаштво у Вуперталу покренуло је истражни поступак у случају једне пацијенткиње која је, због хитног здравственог случаја, требало да буде примљена у Универзитетску клинику у Диселдорфу, али тамо нису могли да је приме, па је пребачена у Вупертал где је захват обављен са закашњењем. Пацијенткиња је умрла, а истражни органи сада истражују да ли је то кашњење узрок смрт.

У случају да јесте, истрага за убиство из нехата окренуће се против особа које су хаковале комплетан рачунарски систем диселдорфске болнице због чега пацијенткиња, заједно са стотинама осталих, није могла да буде примљена.

Министарка науке савезне покрајине Северне Рајне Вестфалије, Изабел Пфајфер-Поенсен у четвртак је потврдила да је Универзитетска болница у Диселдорфу, односно њена хитна служба била мета напада хакера.

Они су прво најавили да ће тражити новац, али су, након што је полиција с њима успоставила контакт, клиници послали безбедносну лозинку за поновно "откључавање" рачунарског система који је био блокиран данима. До потпуног успостављања рачунарског система "проћи ће недеље", како је пријавила управа клинике.

Најчуднији детаљ у причи о хаковању је да уцењивачи у првом писму нису постављали конкретне новчане захтеве и да су, када су им се власти јавиле, одмах дали кључ помоћу којег се рачунарски систем поново успоставља. То надлежне наводи на теорију да је Универзитетска клиника била случајна жртва, а да су уцењивачи-хакери у ствари хтели да уцене Универзитет Хајнрих Хајне у Диселдорфу.

Нови напад могућ у сваком тренутку

Хакери су упали у систем преко једног програма који је, како је речено, уобичајен и распрострањен на тржишту. Савезном уреду за безбедност у информатичким системима (БСИ) грешка у софтверу позната је од почетка ове године и у сарадњи с произвођачем софтвера и погођеним установама покушавају да ту рупу у заштити поправе.

По свему судећи, напад на рачунарски систем клинике могао је да буде избегнут да је управа болнице реаговала на време, односно да је актуелизовала програм, што би затворило опасну рупу у безбедности.

Локална демохришћанско-либерална влада најавила је да ће болницама ставити на располагање већа средства за кибернетичку заштиту. Међутим, проблем је и премало стручног особља у установама као што су клинике. Најновији случај поново је на видело изнео старе проблеме са безбедношћу осетљивих података пацијената. Не ради се, наиме о првом нападу такве врсте: 2016. су хакери на неколико недеља паралисали ИТ-систем једне болнице у Нојсу.

Притом болнице у Немачкој спадају у тзв. критичне делове инфраструктуре и захтевају посебан третман. Зато је њима потребна посебна заштита и ИТ-структуре.

"Теоретски, овакав напад какав смо сада доживели у Диселдорфу може да се догоди у сваком тренутку", рекао је за јавни сервис WDR Норберт Полман, професор на Вестфалијској високој школи

Он каже да су остале критичне установе, попут снабдевача енергијом, много боље опремљене од болница.

"Болнице полажу много енергије у то да пронађу квалитетне лекаре, али не и ИТ-особље. Болнице су предуго спавале када је реч о кибернетичкој безбедности", закључује професор Полман, а преноси DW.

(Дојче веле)