Ransomware slows North Carolina county government to a crawl

December 7 2017, by Jonathan Drew

Mecklenburg County Manager Dena Diorio speaks at a news conference at the Government Center about the hacking of Mecklenburg County's servers in Charlotte, N.C., Wednesday, Dec. 6, 2017. A $25,000 ransom in bit coin was being sought for the files being held. County officials said late this afternoon they are not paying the ransom. (Diedra Laird/The Charlotte Observer via AP)

A cyberattack slowed county government to a crawl Wednesday in North Carolina's most populous metro area as deputies processed jail inmates by hand, the tax office turned away electronic payments and building

code inspectors switched to paper records.

Data was frozen on dozens of Mecklenburg County servers after one of its employees opened an email attachment carrying malicious software earlier this week.

County manager Dena Diorio said late Wednesday that the county will not pay the $23,000 demanded by the hacker believed to be in Ukraine or Iran. Diorio said it would have taken days to restore the county's computer system even if officials paid off the person controlling the ransomware, so the decision won't significantly lengthen the timeframe.

"I am confident that our backup data is secure and we have the resources to fix this situation ourselves," said Diorio.

In the meantime, county departments were scrambling to conduct business without access to digital records.

"We are slower, but we are up and running," Diorio said.

The county of more than 1 million residents includes Charlotte, but the city government appears not to have been compromised by the attack. The state's largest city issued a statement that its separate computer systems have not been affected and that it severed direct connections to county computers.

The computer problems haven't affected the processing of emergency calls because they are handled by the city, said Mecklenburg County Sheriff's Office spokeswoman Anjanette Flowers Grube.

Mecklenburg County Manager Dena Diorio speaks at a news conference at the Government Center about the hacking of Mecklenburg County's servers in Charlotte, N.C., Wednesday, Dec. 6, 2017. A $25,000 ransom in bit coin was being sought for the files being held. County officials said late this afternoon they are not paying the ransom. (Diedra Laird/The Charlotte Observer via AP)

But it's caused delays for the county jail and disrupted other county services ranging from domestic violence counseling to tax collection. Sheriff Irwin Carmichael said it's taking longer to manually process arrestees, as well as inmates due to be released.

Calls to a county domestic violence hotline are rolling straight to voicemail, so counselors are checking messages every 15 minutes, officials told reporters. And the social services department is working to recreate its daily itinerary of 1,600 rides for elderly patients with

medical appointments. Recurring appointments that account for most of the rides are less of a problem than those for patients who make one-time reservations.

Patty Eagan, director of Mecklenburg County Social Services, said there are "300 trips that are medical demand, and that's when someone has scheduled a trip a week ago, two weeks ago. We are not able to see what trips have been scheduled."

Meanwhile, payments to the tax office must be made with a check, cash or money order, and code inspectors are slowed down by using paper records, according to a list of affected services.

Diorio said county computers began to suffer Monday from the attack, which was publicly revealed the next day. A forensic examination shows 48 of the county's 500 servers were affected, Diorio said, adding that county government officials believe that the hacker wasn't able to gain access to individuals' health, credit card or social security information.

The compromised servers have been quarantined, and even potentially healthy parts of the system were shut down to avoid spreading the malicious program, said Keith Gregg, the county's chief information officer. But without getting the compromised servers unlocked, the county will have to rebuild significant parts of the system.

Diorio said county technology officials will use backup data from before the ransomware attack to restore the system, but the rebuild will take "patience and hard work."

A security expert said cyberattacks on local governments aren't unusual. For example, a hacking attack in late 2016 on San Francisco's mass transit system led its operators to allow free rides over part of a weekend because of data problems.

Mecklenburg County Manager Dena Diorio speaks at a news conference at the Government Center about the hacking of Mecklenburg County's servers in Charlotte, N.C., Wednesday, Dec. 6, 2017. A $25,000 ransom in bit coin was being sought for the files being held. County officials said late this afternoon they are not paying the ransom. (Diedra Laird/The Charlotte Observer via AP)

Ross Rustici, senior director of intelligence services at the firm Cybereason, said ransomware schemes against local governments make the news every couple of months, but that they often tend to be smaller, rural areas. He said local governments are "easy targets" because of their older equipment and software.

He said businesses and local governments often pay the ransom because other means of recovering the data can be even more expensive.

"Once you're in that situation, you really have no good option, so a lot of people and companies end up paying," he said.

Citation: Ransomware slows North Carolina county government to a crawl (2017, December 7) retrieved 18 July 2024 from https://phys.org/news/2017-12-ransomware-north-carolina-county.html