Deadline looms for decision by hacked North Carolina county (Update)

December 6 2017

Deputies processed arrests by hand and building code officers used paper records Wednesday as one of North Carolina's largest counties considered how to respond to a hacker who froze county servers and is demanding ransom.

Mecklenburg County Manager Dena Diorio told reporters that officials face a deadline of 1 p.m. Wednesday to decide whether to pay a ransom of two bitcoin, or more than $23,000. Bitcoin is a digital currency used around the world and favored by some hackers because it can often be exchanged online anonymously.

Diorio said county electronic files have essentially been frozen after the attack that started when a county employee opened an email attachment carrying malicious software.

The county of more than 1 million residents includes North Carolina's largest city, Charlotte, though that municipality appears not to have been directly affected by the hack. The city released a statement Wednesday that its separate computer systems have not been affected and that it has severed direct connections to county computers.

Mecklenburg County Sheriff's Office spokeswoman Anjanette Flowers Grube said in an email that deputies are manually processing suspects who have been arrested because its computer system was affected. The sheriff also announced that the county jail's website wasn't displaying inmate search information that's normally easily accessible.

But Flowers Grube said the problems don't extend to processing emergency calls, which is handled by the city of Charlotte. City fire and police officials didn't immediately return messages seeking comment.

The county issued a statement on Twitter Wednesday asking residents to contact county offices before visiting to see whether they are offering services. Diorio said, for example, that the county's code enforcement office would have to rely on paper records until the outage is fixed because employees there can't access the electronic files they normally rely on.

Diorio said the county hadn't ruled out paying the ransom, but understood that could be risky.

"If you pay the bitcoin, there is always a risk they won't give you the encryption key," she told reporters.

She said the hacker didn't gain access to protected information on people's credit card data, health information or social security numbers.

An expert on cyber security told The Associated Press that it's not uncommon for municipalities to be hacked with ransomware. 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.

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 they typically have older equipment and software than corporations or the federal government.

He said it's not unusual for businesses and local governments to pay the ransom. He said it's often more costly to try to recover the data unless technology officials are proactive about safeguards including frequent data backups.

"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: Deadline looms for decision by hacked North Carolina county (Update) (2017, December 6) retrieved 25 April 2024 from https://phys.org/news/2017-12-north-carolina-county-servers-hacked.html