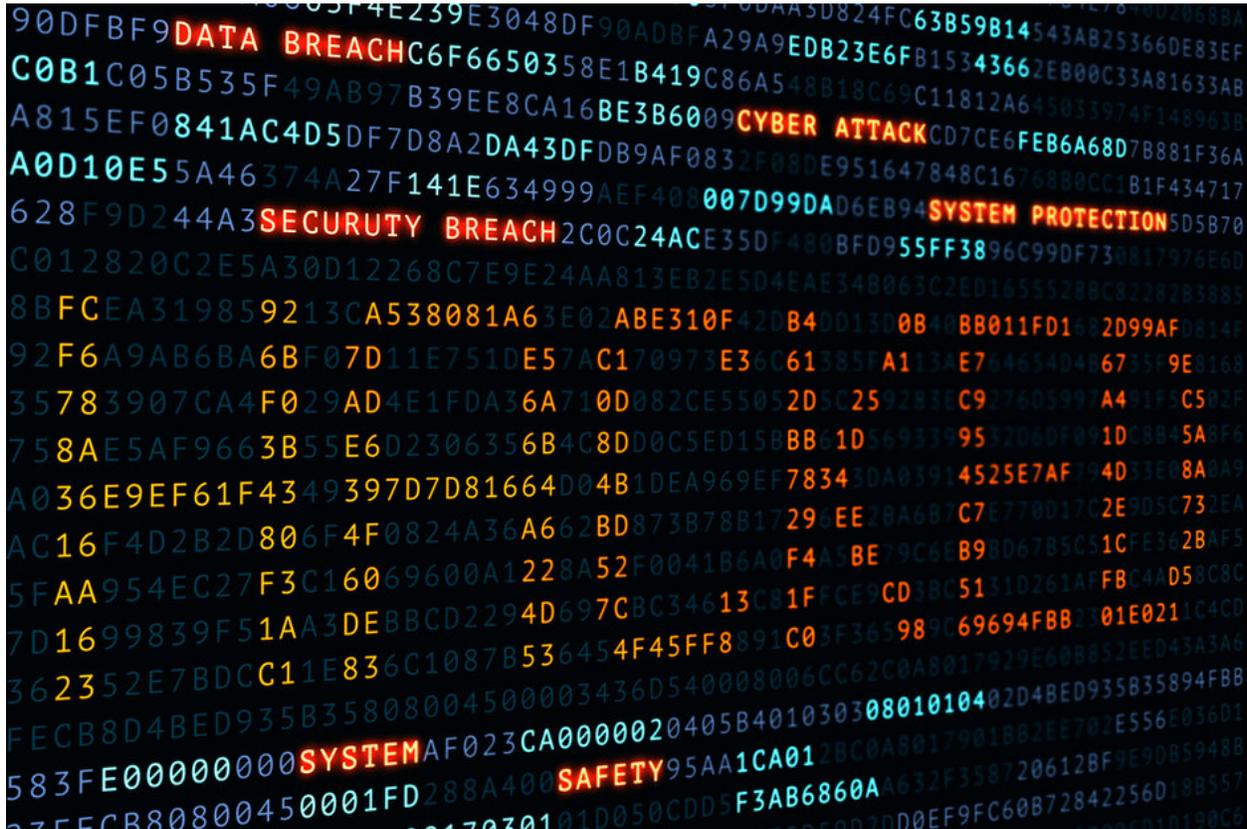


North Carolina County Announces Full Recovery from Ransomware Attack

March 20, 2018



(TNS) — A month after Davidson County systems were infected by a ransomware virus, County Manager Zeb Hanner said that all servers are up and running while the FBI continues to investigate the incident.

It was originally believed the process could possibly take months to sort through. The source of the virus hasn't been identified, but Hanner said it probably was not through an email.

"There's nothing we know of that's not running right now," Hanner said. " ... We got it up a little faster than we thought we could. They did a fantastic job."

In the early morning of Feb. 16, officials realized that 911 Emergency Communications was experiencing suspicious activity. It was later discovered that all county systems had been affected by a ransomware virus known as Samas.

At the time, the virus impacted approximately 70 of the county's 90 servers and an unknown amount of desktop computers and laptops. The phone systems were affected, as well.

The hackers asked for an undisclosed amount of Bitcoin, a type of cybercurrency gaining popularity. Hanner said he is still unable to disclose how much the hackers asked for due to the ongoing criminal investigation by the FBI.

Hanner said all of the county's Information Technology department and officials from the insurance company assisted with the restoration process. The county manager noted that no data was stolen from the county's systems.

Hanner said that while the systems were down initially, the Lexington Police Department helped the Davidson County Sheriff's Office. Thomasville, Archdale, U.S. Rep. Ted Budd's office, Rowan County and the North Carolina Association of County Commissioners were all among the agencies that offered assistance while the county worked through the problem.

A similar incident occurred to Mecklenburg County's computer systems in December. According to the Charlotte Observer, a foreign-based hacker gained access to a government employee's log-in information to launch the ransomware. The hackers reportedly asked for \$23,000 in return for restored access, which county officials refused.

A couple of weeks ago, it was revealed that a hacker invaded Catawba County's human resources and payroll system in October and compromised the information of 187 employees.

Hanner said that every employee already completes cyber training each year that teaches how to look for phishing emails and that emails from an external source are labeled in the subject line. He added the county is looking to invest in measures to prevent future incidents.

"I know Joel (Hartley, the county's chief information officer) in the upcoming budget is going to ask for a few pieces of equipment that will probably be even more proactive in trying to seek out attacks," Hanner said. " ... We'll continue to tighten down."

Hanner said he'd advise any other government agency to keep checking systems, be cognizant of firewalls and always try to take a proactive approach.

The county manager said this type of hacking is not a matter of if, but a matter of when.

"This is the world we live in, and people are constantly looking for ways to get into other people's systems. Instead of home invasion, it's a cyberinvasion," Hanner said. " ... These guys do this and they are highly intelligent folks that know how to do this stuff."

©2018 The Dispatch, Lexington, N.C. Distributed by Tribune Content Agency, LLC.