Fallout from cyberattack on Atlanta computers still unclear (Update)

March 23 2018, by Kate Brumback

More than 24 hours after a ransomware cyberattack targeting the city of Atlanta's computer network was discovered, the fallout still wasn't clear.

Atlanta city officials announced Thursday afternoon that the city's information security team had noticed "something that looked peculiar" on the server about 5:40 a.m. that day and began an investigation. Some city data was encrypted, essentially held for ransom by the attackers.

The attack caused an outage for some internal and customer-facing applications, including those used to pay bills and access court information, city Chief Operating Officer Richard Cox told reporters at a news conference Thursday. But it did not affect the public safety department, water department or Hartsfield-Jackson Atlanta International Airport, he said.

The airport shut down its Wi-Fi network and the systems that provide flight information and security checkpoint wait times on its website "out of an abundance of caution," spokesman Reese McCranie said in a phone interview Friday.

"We don't want to open up the airport to any possible cyberattack," he said, adding that the airport's technology staff was working to harden its infrastructure to make sure it's not vulnerable.

A city spokesperson said Friday that there was no new information available.

It was not immediately clear whether any personal information had been compromised, but Mayor Keisha Lance Bottoms urged city employees, residents and others whose data may be in the city's system to monitor their bank accounts and to take proactive steps to protect their personal data.

The city is working with federal agencies, including the FBI and the Department of Homeland Security, as well as private sector partners, to fix the problem, Bottoms said.

Mark Ray, a former FBI cybersecurity investigator who's now managing director and head of digital investigations for Nardello & Co., said the agency's primary goals are to stop an attack and find out who's responsible.

The agency's first step would be to give practical advice such as isolating the affected systems, preserving and protecting unaffected systems by taking them offline, as well as making sure backups are preserved and secure. Next, the FBI would want to get a sample of the ransomware because it may already have intelligence on that particular malware that could help stop it or it may have a decryption key from a previous attack.

When asked Thursday if the city would pay the ransom demanded, the mayor said the city would seek guidance from federal authorities on the best course of action.

The FBI will never advocate paying ransom, Ray said. There are a variety of reasons for that, including: There's no guarantee the ransomware owner will actually provide decryption after being paid, an organization's willingness to pay can make it a target for future attacks, and sometimes payment results in the unlocking of part of a system but then more money is demanded to unlock more of the system.

But if an organization chooses not to pay ransom and if there is no readily available decryption key, "the alternative is, literally, to slash and burn the environments that have been infected," Ray said. "That's where good backups are critical."

Ransomware exploits known software vulnerabilities, and often organizations that fall victim to such attacks haven't done a thorough job of patching systems regularly, he said.

Municipalities often struggle with basic software updates and patching because they are frequently short on resources, said Ryan Kalember, senior vice president of cybersecurity strategy at the security company Proofpoint.

The Atlanta attack bears the hallmarks of the SamSam ransomware, and what the city's information security team likely saw was something trying to log on from outside the organization, he said.

Unlike most ransomware, which accesses a network when someone clicks on link in a phishing email, SamSam indiscriminately searches the internet for vulnerable servers, Kalember said. Once it finds a foothold—often by exploiting a weak password or one that doesn't get changed often—it gets inside a system and starts to spread.

If it is SamSam, there may be a bit of good news because it typically encrypts the information in place and demands a ransom to restore access to it rather than stealing the information, Kalember said.

"It's a wakeup call and it's not ultimately that harmful so there's a clear silver lining for municipalities" because it could motivate the city to put resources and political will behind making its networks more secure, he said.

Citation: Fallout from cyberattack on Atlanta computers still unclear (Update) (2018, March 23) retrieved 25 April 2024 from https://phys.org/news/2018-03-atlanta-airport-precautions-cyberattack-city.html