4-StateScoop-Atlanta

Atlanta was not prepared to respond to a ransomware attack

Share

Written by Benjamin Freed Apr 24, 2018 | STATESCOOP

A month after the SamSam ransomware virus infected its computer systems, Atlanta's city government still struggles to provide several services to its residents *[Disappointment]*. Water and sewer bills can't be paid online or over the phone, and business licenses can only be obtained in person *[Disappointment]*. Public Wi-Fi at Hartsfield-Jackson International Airport, the country's busiest airport, was down for two weeks *[Disappointment]*. City council members reported losing decades' worth of correspondence *[Disappointment]*. The municipal courthouse only regained the ability to schedule traffic-ticket hearings on April 16.

Atlanta officials may eventually give full accounting of how the March 22 ransomware attack was allowed to happen, and why the recovery process has been so slow and out of the public view *[Disappointment]*. (The city last issued an official update on March 30.) But the hack hit just the right conditions to sow mayhem: In the weeks since officials were locked out of their systems for a $51,000 ransom demand, it's been revealed that Atlanta's municipal IT was woefully disorganized and outdated *[Disappointment]*. Couple that with the recent swearing-in of Mayor Keisha Lance Bottoms, who by her own admission had not devoted much attention toward cybersecurity, and Atlanta became a ripe target for digital bedlam.

As recently as January, the city auditor was excoriating officials for a lax approach toward cybersecurity *[Disappointment]* that left the government with obvious vulnerabilities, obsolete software and an IT culture driven by "ad hoc or undocumented" processes, according to a report published that month by the auditor's office. Now, the city is scrambling to dig out from arguably the highest-profile ransomware incident on U.S. soil yet, shelling out nearly $2.7 million in emergency contracts to IT consultants and crisis managers.

Not everyone is looking for someone to blame, though. Amid all the frustration that the cyberattack has caused, there's one push for Atlanta to conduct a "blameless" review of the episode *[Positive]*. But that seems like something that's still a long way off from happening. Whatever the case, the attack was not surprising to cybersecurity experts.

"Atlanta is a fairly typical path," said Max Kilger, a business professor who specializes in cybersecurity at the University of Texas at San Antonio. "These guys seem to be targeting organizations that work for the public good *[Neutral]*. There's an urgency when a city gets taken down. The ransomware people are basically counting on that to leverage a payment out of these targets."

Better to spend now than pay later

By all known accounts, Atlanta hasn't paid up, though the mayor's public remarks about it have been inconclusive. "Everything is up for discussion," Bottoms said six days into the hack. The involvement of the FBI, which recommends ransomware victims refuse their attackers' demands, suggests Atlanta hasn't given in.

Kilger said a city as large as Atlanta, with a $2.1 billion budget, is a tempting target for ransomware operators because the ransom demand is so paltry compared the city's pocketbook. Even if Atlanta won't pay, the hackers behind the SamSam ransomware are still running a tidy operation — collecting nearly $850,000 since their first attack in late 2015, according to analyses of the SamSam group's bitcoin wallet . That includes payments from ransomware victims that did pay the bounties to recover their data, including Hancock Regional Hospital in Indiana and Yarrow Point, Washington, an affluent town of 1,000 residents just east of Seattle.

But in those cases, the targets went against the FBI's advice. The bureau recommends against acceding to ransom demands for the simple reason that a ransomware victim has no guarantee that its attacker won't "shoot the hostage" anyway. "Paying a ransom doesn't guarantee an organization that it will get its data back — we’ve seen cases where organizations never got a decryption key after having paid the ransom,” the FBI advises.

If there’s money going anywhere, it’s to consultants. In the month since the hack, Atlanta has doled out more than half a dozen emergency contracts to cybersecurity firms like Secureworks, Fyrsoft, and CDW, and consulting services from Ernst & Young and Edelman to manage the public response *[Rebuild]*. In Colorado, where a SamSam attack in February took out internal systems at the state’s transportation department, officials have spent between $1 million and $1.5 million on recovery so far. *[Rebuild]*

Government IT officials might find it’s better to spend more money up front hardening their cybersecurity *[Rebuild]*, rather than shelling out after a hack.

“If I were an executive, I would look at the risk equation,” said Walter Tong, a security architect at the Georgia Technology Authority, which manages the state’s IT infrastructure. ”Is it worth spending the money or paying the ransom? I would not like to be in that kind of position.”

IT complacency

Tong’s office is not working on Atlanta’s recovery; he said it doesn’t offer the kinds of recovery services the city needs right now. But he said he knows the job of rebuilding the city’s computer systems will be a long one.

“It takes a while to rebuild and reconstruct applications and network devices,” Tong said. “Hackers choose targets and they find ways of getting there, whether it’s to cause a disruption of service or destruction of data, or both.”

Unlike other ransomware programs that take over networks when a user opens a phishing email or inadvertently runs a malignant program, SamSam infiltrates systems with brute-force attacks like guessing weak or default passwords until one breaks through. SamSam often targets Java-based application servers or Microsoft’s Remote Desktop Protocol.

Tong said his office often looks for those kinds vulnerabilities in network settings and older devices. Had Tong's team examined Atlanta's systems, they would've found those conditions in abundance. The city auditor's January report found nearly 100 government servers running on Windows Server 2003, which Microsoft stopped supporting in 2015.

"You can spend a lot of time on educating, making sure your network devices are patched and secure," Tong said. "But once it happens, you have to have an instant response plan."

The January audit report suggests Atlanta was nowhere near ready to deal with a cyberattack. Monthly scans conducted over the course of the audit, found between 1,500 and 2,000 security vulnerabilities in Atlanta's systems. In fact, the number of IT security flaws grew so large, that city agencies slid into a habit of inaction, the audit stated *[Disappointment]*.

"The large number of severe and critical vulnerabilities identified by the monthly vulnerability scan results metric has existed for so long the organizations responsible for this area have essentially become complacent and no longer take action other than to update the monthly report *[Disappointment]*," the document reads. "The significance of such a backlog of severe and critical vulnerabilities without corrective actions is evidence of procedural, technical or administrative failures *[Disappointment]* in the risk management and security management processes."

Don't play the blame game

Whether the hackers who hit Atlanta knew it at the time, the ransomware arrived less than three months into the term of a new mayor who admitted after the hack that cybersecurity had not been one of her administration's priorities. *[Diminish]* That was a shift from her predecessor, Kasim Reed, who often played up Atlanta's emergence as a hub for the cybersecurity industry: The city is home to companies like SecureWorks and Bastille, and Reed went on trade missions to Israel to get that country's cybersecurity firms to investin Atlanta. *[Rebuild]* Internally, Reed's chief information officer, Samir Saini oversaw some IT upgrades, like moving city employees from Microsoft Exchange servers to Microsoft's cloud services.

Saini was snatched away by New York Mayor Bill de Blasio in January, leaving Saini's former deputy, Daphne Rackley, as the interim CIO. Then on April 9, Bottoms shook up the city's leadership by asking everyone in her 35-member cabinet, which is still comprised mostly of holdovers from Reed's administration, to submit letters of resignation . Bottoms hasn't announced who she'll be keeping and who she'll be replacing, but the ransomware attack has made the CIO job a crucial one to watch.

"Just as much as we focus on our physical infrastructure, we need to focus on the security of our digital infrastructure," *[Rebuild]* Bottoms said a few days after the hack.

But blame for the ransomware attack and responsibility for making sure it doesn't happen again aren't necessarily synonymous. Code for Atlanta, a Code for America brigade that advocates for better technology in municipal government, wants Bottoms to eventually order a report that avoids assigning blame *[Hope]*.

The idea of a "blameless post-mortem" is widely attributed to developers at the craft site Etsy. In a 2012 post on Etsy's developer blog, John Allspaw, then a senior vice president at the company, wrote that software engineers respond better to errors and accidents when they know there's not an overt threat of punishment.

"[A]n engineer who thinks they're going to be reprimanded are disincentivized to give the details necessary to get an understanding of the mechanism, pathology, and operation of the failure," Allspaw wrote. "This lack of understanding of how the accident occurred all but guarantees that it will repeat. If not with the original engineer, another one in the future. *[Disappointment]*"

Other companies, including Google, have since adopted that model of review after things go wrong. Code for Atlanta believes that model could work in the public sector, too *[Hope]*.

"We want folks in city government to be accountable, but for us it's more about a culture change," *[Hope]* the group's leader, Luigi Ray-Montanez, told StateScoop. "When I was at city hall I saw this poster warning people to be wary of cyberattacks *[Hope]*. It seems like they were aware of internet culture, but obviously mistakes were made.”

Atlanta City Auditor Amanda Noble told reporters when the audit was first publicized that city officials had started to upgrade their IT security when the ransomware attack hit. But the majority of recommendations the audit made are unlikely to be completed until the third and fourth quarters of 2018.

Despite a recent push to make her government more transparent — including plans to create websites on which the public can track city contracts and municipal data — Bottoms hasn’t given an official statement on the ransomware recovery in weeks. Her office has not responded to requests for an update. Rackley, the acting CIO, has not responded to requests for an interview. *[Deny]*

Tong, the security architect for the Georgia Technology Authority, said the city’s current silence might be at the behest of the investigators.

“It’s an active investigation and they likely can’t disclose what’s going on,” he said. *[Neutral]*

The recovery time for a ransomware victim that doesn’t pay off its attacker can be long. The Colorado Department of Transportation was only 80 percent back online six weeks after it was hit by the SamSam virus. Atlanta’s systems have been flickering back on in spurts, with many public services still rolled back to the pen-and-paper era.

Atlanta’s IT professionals and the contractors it’s hired in the wake of attack are scrambling to patch the holes and upgrade to more secure systems. But lingering out there now, for Atlanta and everywhere else, is the threat of more ransomware attempts to come. *[Worry]*

“This is one of many ransomware attacks, and there will be many more,” Kilger, the Texas professor, said. “It’s going to get worse.” *[Worry]*

-In this Story-