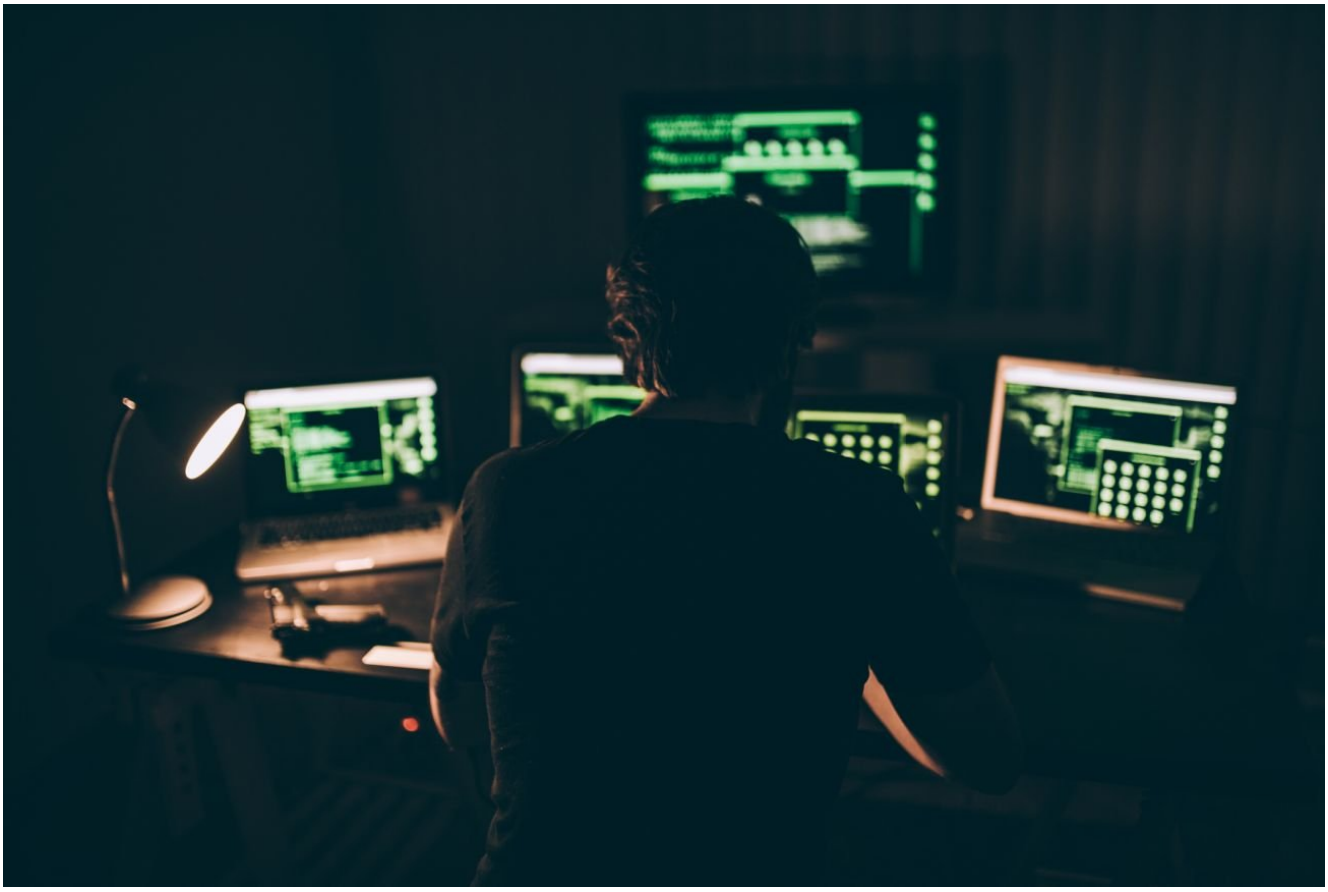
4 Lessons Your Organization Can Take From Atlanta's Ransomware Attack



Ransomware attackers are the muggers of the internet, looking above all else for those most easily victimized.

April 3, 2018 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

In late March the computer system of the City of Atlanta was victimized by a ransomware attack and, 10 days later and counting, the city's computer system is still at least partially gridlocked, with ripple effects experienced in a variety of critical areas. What went wrong, and what can be done to ensure other cities and organizations aren't compromised in a similar way?

On Thursday, March 22, Atlanta Mayor Keisha Lance Bottoms made an announcement in a press briefing that the city's computer network had been compromised by a ransomware attack. The attack encrypted a significant portion of the city's data and the hackers were demanding 0.8 Bitcoin per computer – or six Bitcoin ($50,000) to unlock the entire system.

For those who are unfamiliar with ransomware, it's an attack in three phases. In Phase 1, attackers look for vulnerable servers on the internet, which typically are those with weak passwords or poor security protocols. They aren't usually targeting specific organizations. Instead, they look until they find easy prey.

In Phase 2, the attackers explore the network and look around the hacked server to get their bearings. In this stage, they're trying to identify the most valuable files, databases, email accounts, etc within the server. Phase 3 is the actual ransomware attack that locks out users and demands a payment to restore access. The ransom payment is usually set according to what the hackers believe the organization can pay.

The Atlanta attack was serious enough that many city departments and organizations – including the court system – shut down its computers and went offline for a couple of days. Hartsfield-Jackson Atlanta International Airport, while not directly affected, chose to play it safe, in the immediate aftermath, by shutting down its free Wi-Fi network and certain website functionalities.

For at least six days after the attack, systems that typically enable residents to pay water bills and parking tickets online still remained unavailable. Many police officers were also still filing paperwork by hand.

Mayor Bottoms used strong language to describe the incident, saying, "We are dealing with a hostage situation." Unfortunately for Atlanta, it is a hostage situation they are

ill-prepared to handle.

Related: Ransomware Could Be the Monster If Stephen King Wrote a Novel About Small Businesses

At this point in 2018, it’s inexcusable for any organization – regardless of whether it’s an entire city government or a small business – not to have a robust cyber security strategy in place. Instead of just looking on and shaking your head at the situation brewing in Atlanta, make sure you’re taking this as a valuable opportunity to learn.

Here are four important takeaways:

1. Secure your networks.

The first step is to secure your network. While the City of Atlanta certainly had some security mechanisms in place, they clearly weren’t sufficient. Now (not after the fact) is the time for you to find out whether your defenses are capable of withstanding an attack.

Many companies will benefit from using a virtual private network (VPN), which secures web traffic and provides an additional layer of protection against attacks. Consider looking into this, especially if you have lots of remote workers.

Related: How to Choose a VPN Provider for Your Business

2. Educate employees.

Security mechanisms and layered protection are important, but they don’t mean anything if employees don’t understand how to act. From better password hygiene to the ability to identify risky emails, employees need to play a bigger role.

3. Stay up to date.

It’s one thing to align your company with various cyber security solutions, but you can’t just plug them in and leave them alone. Cyber criminals are constantly tweaking their methods and coming up with new attacks. In response, you must continually update your own security measures.

Related: How to Maintain Security When Employees Work Remotely

4. Don’t pay the ransom.

When a person is kidnapped and a ransom note is delivered to the individual’s parents, spouse, or a local government, the general rule of thumb is that you don’t pay the ransom. Or, if you do, you make sure it’s done quietly.

With ransomware, there’s rarely a situation in which you ever consider paying the ransom. For starters, there’s no guarantee that you’ll ever get your files back. Secondly, many ransomware attacks actually have poor cryptography implementations, which means you can pay someone far less to actually correct the problem and retrieve your files.

Related: Is Paying up the Only Response to Ransomware?

During the first few months of 2017, ransomware attacks were up 250 percent over the previous year. They continued to be a major problem throughout the year and the issue has spilled over into 2018.

Cyber security strategies aren’t optional. Your organization will be exposed if it doesn’t take security seriously. And as the City of Atlanta recently discovered, you can never be safe enough.

What, if anything, are you doing to protect your organization moving forward?

https://www.entrepreneur.com/article/311312