Bond Case Briefs

Municipal Finance Law Since 1971

Atlanta's Ransomware Isn't an 'Isolated Incident'

COMMENTARY | Symantec's Tim Hankins outlines the continued prevalence of ransomware attacks, and what it means for governments as they consider their level of cybersecurity.

For nearly a week, a ransomware attack crippled the City of Atlanta, sending government operations back 30 years in the process. Residents could no longer pay bills online, police officers filled out reports by hand, and all unscheduled court cases were postponed until further notice.

That, of course, was just the technology side of the equation.

"I just want to make the point that this is much bigger than a ransomware attack," Atlanta Mayor Keisha Bottoms said six days after the attack as the city began to get back online. "This is really an attack on our government, which means it's an attack on all of us."

Sadly, this is not an isolated incident.

In this year's Symantec Internet Security Threat Report (ISTR) the number of ransomware attacks remained near the all-time high set in 2016. While the number of attacks is important, the more notable revelation was how ransomware attacks continue to evolve. There were 28 new ransomware families detected last year, and the number of overall ransomware variants increased by 46 percent. The ISTR showed that while ransomware, overall, has slowed its growth, it still remains a dangerous threat that can cause tremendous damage.

The number of ransomware attacks has grown at a considerable rate in recent years. We've seen a significant uptick of ransomware attacks impacting healthcare organizations, and state and local government is trending right along. In April 2018, the Riverside, Ohio police and fire departments became victims of ransomware. City manager, Mark Carpenter, implied that a third-party held, or is holding, the city's data hostage in exchange for a ransom, often paid in bitcoin or another cryptocurrency.

Local agencies, especially the police and fire departments, can't accept downtime. After all, lives hang in the balance. With mission critical functions being impacted during a ransomware attack, it's easy to understand the temptation to comply with demands for ransom. However, the FBI and cybersecurity professionals generally agree paying ransoms is a bad idea. First, there is no guarantee that the hackers will release the data once paid. There is no honor amongst thieves, after all. Second, this quick payday incentivizes these hackers to continue what they are doing. Some organizations have even budgeted funds in order to pay off ransomware attacks.

In some ways it is surprising that state and local governments, not to mention healthcare organizations, academic organizations and non-profits, do not find themselves subject to more ransomware attacks. These governments hold a tremendous amount of personal information about citizens and often have significantly higher financial benefits to hackers than individuals or small businesses, and many operate without a robust cybersecurity posture.

For example, the Roseburg Public Schools System in Roseburg, Oregon, suffered an attack this May of its computer system. The FBI, which was brought in to investigate the case, believes the attack occurred through a complex method using remote desktop protocols, rather than through malware attached to an email sent to someone within the district. According to the FBI, these types of attacks are occurring at increasingly frequent rates, targeting schools, businesses and government entities.

Unfortunately, no jurisdiction is out of harm’s way. In fact, many states are finding themselves victims of multiple attacks. On March 9, 114 servers within Connecticut’s judicial system were impacted by a ransomware attack, the second ransomware attack aimed at the state government. Two weeks earlier, the Connecticut Department of Administrative Services reported that a virus resembling the Wannacry ransomware infected about 160 computers in a dozen state agencies.

Fortunately, in both Connecticut attacks, the virus was detected and mitigated early. And, if state and local organizations follow good cybersecurity practices, they too can find themselves avoiding the often costly effects of a ransomware attack.

So, what should an organization do to prevent ransomware attacks? For many it simply starts with good cybersecurity practices. Some of these are simple steps like ensuring systems are patched and backed up regularly, that “endpoints” are protected, and appropriate email security is in place.

However, more advanced techniques may be necessary in many public sector environments. Being able to combine basic cyber hygiene and advanced capabilities into an integrated cyber defense platform will allow agencies to uncover, prioritize, investigate and remediate ransomware attacks across their endpoints, networks and email platforms.

Having a good cybersecurity architecture in place not only blocks ransomware, but it blocks all accounts. Ransomware has become a popular form of attack because it works. If organizations take the steps to protect their systems, governments can greatly reduce their risk of ransomware and other malicious cyber attacks.

Route Fifty

By Tim Hankins

Tim Hankins is vice president of government, health and education at Symantec, a Fortune 500 company specializing in cybersecurity.

JUNE 22, 2018