Alabama County Foils Ransomware Attackers Attempts to Extort

Customer: St. Clair County, Alabama
Industry: Public Sector/Government
Location: Ashville, Alabama
Solution: DataGard - ThinkGard's Total Data Security

In 2020, over 100 cities and municipalities across the U.S. were hit with ransomware, resulting in hundreds of millions of dollars paid out in ransom. St. Clair County, Alabama, was one of those municipalities that got hit.

We caught up with John Myers, IT Assistant Manager at St. Clair County, who shared his recent ransomware experience.

It was just months after the county had dedicated a full time IT staff that they were attacked. Previously, the St. Clair County School System had handled the technology needs for the county. After the two departments separated, St. Clair brought in IT Manager Glenn Morgan and IT Assistant Manager John Myers. That's when they started using Veeam for Backup and Disaster Recovery according to Myers. "It was okay, but we had a couple of instances where we had to restore and we weren't satisfied with the recovery time. It was a bit clunky and it would take a lot of effort and time to bring things back up. We had our ears to the track so to speak, and that's when our Managed Service Provider (MSP) at the time introduced us to ThinkGard. When we started talking to ThinkGard, we got super excited about being able to back up to 2 bicoastal data centers as well as getting our data up in the cloud. ThinkGard offered all the things we were looking for, including a written and yearly tested DR plan and they were local (Which we really liked) so we implemented the ThinkGard solution in October of 2017.

The Attack

It was September 21st in 2020 "We got a phone call that Monday night at about 7 pm from our Sheriff's Department saying their machines were going down. They said that there was a message that popped up on the screen, it was an html file that notified everyone that it was ransomware. "

How did you respond?

"Do you mean after crying? Seriously, I was at home when I got the call and the first thing I did was to connect in through our VPN

> *"It happened on Monday and Friday was payday for 300+ employees of the county."*

to see how many servers had been affected. I think I got to a total of 3 before I made the call to ThinkGard to confirm the attack and to confirm that the backups were good. We called our security firm too. Then we notified all the elected officials and the County Administrator. We basically spent that Monday night into the Tuesday morning looking at and evaluating the damage to see how it got in. Basically, trying to understand the footprint or find a signature. We attended a county commission meeting the next morning and that was when we advised the commission of the plan that we had to get back up and running.

It was pressing on us to do something fast. Because it happened on Monday and Friday was payday for 300+ employees of the county. We had the added pressure of making sure that payday wasn't delayed. It's really what motivated us to get it back up so quickly."

Assessing the Damage

We didn't find any evidence of phishing or password theft, so one of the first things we did that night and going into Tuesday night was to verify that we didn't lose any data. Security then ran a log to see if any data was exfiltrated. They were able to crunch and verify that nothing escaped. And that was the whole gambit from emails to HR to our inmate data etc.

Taking Action

Our order of process was that we basically, with Michael & Adam at ThinkGard's help, we were able to bring up our payroll systems first. We set it up in an environment by itself completely disconnected from our original network. Once that was done, we had a lot of help from the server and network guys who came in from the Department of Education. We had a brain storming session about our plan of attack. We got our network domain controller up and running, we built a new one and got the main one back up and running to get the network re-established. After that we made a plan for our endpoints. It was decided that because it was a rare ransomware, (in that most ransomware, when they infect a network, they sit dormant gathering info to see how networks work) what we found is that this was an instant hit. Because we spun up some servers from the previous day from our backups in a standalone environment and found no evidence or signatures or anything of that nature. So, once it hit, it didn't linger or hangout. It just basically propagated itself quickly as it could.

"We found out that the that this was a variant of a strain that was released in 2017. It had a very similar signature and once we found that signature, we were advised to do a military wipe on all our endpoints and just reload them. Which is what we did. As far as our servers, we just rolled them back a day."

"There was one physical machine we had to bring back up the rest were virtual and I have to say Thinkgard's bare metal restore on Physical machines is pretty cool!"

What ThinkGard has established from the top down is amazing. I bother Adam all hours of the day and after hours. The ThinkGard team was always there and making sure we understood exactly what was going on. It was a horrible thing to have happened, but you guys made the bitter taste of it go away when we saw how successful it was bringing up our main data structure."

It was a horrible thing to have happened but you guys made the bitter taste of it go away when we saw how successful it was bringing up our main data structure.'

Has the solution yielded a Return on Investment?

When we asked if there was a particular ROI with ThinkGard's solution, John said, "Thinkgard's system is a huge time saver. We still do our due diligence by looking at the backups every morning and we can see how things are processing but just knowing that if something hiccups, just one time, we get instant notifications. There's no delay. It saves us money too. at least it saves us from loss of revenue. Our revenue is segmented in a way where each department has a server that's protected by you guys and the ability to have those come back up so quickly, not only benefits the county in terms of revenue but, it enables our citizens to continue pay their property taxes, renew their vehicle tags, look up their court dates. It even helps our road department know where to go to fill a pothole. It keeps our first responders online and helps public transportation who assists Citizens in St. Clair County who are in need of getting to their doctor appointments or buying their groceries. Our servers affect all those services. Also, if the court servers are down and people are getting paid just to sit around and wait, we'd lose a lot in revenue. That's why having a proven DR system is needed in just about any environment. The fact that we can quickly spin up a system if it goes down, keeps us running without interruption.

Mitigating Future Risk

"The moving to Office 365 will shed the need of having onsite Exchange servers. It'll also give us protection with OneDrive and email being handled through Microsoft. Had we had it already, we would have still had email for the end users. We implemented a laundry list of policy and security changes. We put new rules into place on how traffic navigates and how executables get populated and ran. There were a multitude of changes to help mitigate the risk of it happening again. I'm not going to say it won't happen again. Lord willing it won't happen again on this network but, if it were to happen again, we feel like we have some things in place that will stop it. Hopefully, by implementing all these changes, the hackers will take a look and just decide to go somewhere else because it's just not worth their effort."

There's not 100 percent protection because as long as you have end users in technology, the weakest link is going to be at least, one of them. You have to train them and teach them to be suspicious of everything because just one lapse in judgement will open the door. The best thing you can do is ask yourself, if an endpoint lets something in, what's the worst thing that could happen? And that's where we are now trying to mitigate that scenario. It's like having a 30,000 dollar door on your building and your back window is wide open. That can happen from using an older windows machine that you overlooked or someone fell asleep at the wheel and clicked a malicious email. The trick is to prepare for the worst and hope for the best. You can add several layers of security and all it takes is one person to make a mistake. What it boils down to is if you get so particular about your security that you interrupt productivity, then who's winning? Your users still have to stay productive. And you still have a responsibility to keep everyone safe.