Highlights from a Recent Webcast on Ransomware

BUILDING RESILIENCE AGAINST RANSOMWARE

Focus on the Left of the Boom and Back Up Files before Any Attack

On Friday, March 6, 2020 the city of Durham, N.C. was hit with a ransomware attack. Durham had a hardened backup system from Rubrik in place so their systems were only down for a short period of time. They were able to get critical city services such as 911 back online very quickly. Over that weekend the city's IT staff was able to recover all of its key services and they were completely up and back in business by Monday morning. Durham's story is somewhat unique in that it didn't have any long-term damage. That's definitely not typically the case.

Ransomware is one of the main threats facing both public and private organizations across the world. Last year, for example, the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) received 2,047 ransomware complaints, an increase of 38% year-over-year. The average recovery time of a ransomware attack is 7.3 days, according to research firm Forrester. Some organizations simply can't recover at all.

When COVID-19 hit, cybercriminals came out and announced they would reduce the number of attacks they launched and completely bypass health-related organizations. While there was a precipitous drop in ransomware attacks, the cyber gangs' self-imposed shackles recently came off, and ransomware incidents have started rising, with attackers using fear of the coronavirus as an attack vector. In addition, targeted attacks, also called big game hunting, are up, and cyber criminals are shifting their strategies, threatening to expose data, rather than just encrypt and delete it.

> "You can do everything right, and still get attacked. It's always going to be coming back to, 'Can I recover? And how quickly can I recover?'"
>
> *— Rebecca Fitzhugh, principal technologist and director of developer relations at Rubrik.*

Companies and agencies are getting hit harder, and the end results are getting worse," explained Rex Booth, Cyber Threat Analyst at the Cyber and Infrastructure Security Agency (CISA) in the U.S. Department of Homeland Security. He was speaking during a webcast called "Avoiding the Ransomware Trap with Protected Back-Up and Cloud Data Management."

"The sophistication of the threat isn't the relevant factor for a victim," he said. "It's the magnitude of the impact, and through that lens, ransomware is a big deal. Being unable to function, losing the progress that you've made since your last backup, halting productivity. In many circumstances, [these issues are] far more devastating than the Chinese or whomever stealing your corporate intellectual property."

Figuring out how to not just recover from an attack, but prevent one completely is where organizations and agencies must concentrate their efforts, and it's simply not enough to engage in the same strategies that worked in the past, Booth said.

Everything we do exists on a timeline and for cybersecurity, technologists as a whole look at actions relative to a bad event as either left of boom or right of boom. Sometimes you can fix things right of boom, or after something goes wrong. IT can detect the adversary once they're in a network and evict them, or can reroute traffic around a dead gateway. It's possible to "remotely brick stolen phones and laptops, but there are lots of solutions that simply don't exist right of boom," CISA's Booth explained. "You can't reclaim the confidentiality of sensitive papers posted on Pastebin and you can't recover lost files with no backup.

There's no magic wand that we or anybody else has to reverse the ransomware -- the impact -- once it's occurred."

Agencies like CISA can come in and perform analysis on the ransomware so that agencies understand what they're dealing with. Occasionally, there may be keys out that can help unlock a specific variant but generally speaking, that's not going to be the case, Booth said.

However, by concentrating on the time to the left of the boom – before cybercriminals get in – you can reduce the chance of ransomware making it into your infrastructure. Booth said that every agency should be thinking about the following things now to reduce the chances of ransomware infection and improve recovery efforts if the unthinkable happens, including deciding whether or not a ransom will be paid.

The answer to the last point – at least for federal agencies – is typically no. Booth why cyber criminals are more likely to focus on the private sector, as well as state and local governments when they are planning attacks.

Still, it's important for every organization to focus on that time to the so-called "left of the boom," where you can prevent attacks before they happen. Booth was quick to explain that something as simple as employee education can help reduce the number and severity of an attack.

"With ransomware or really any disaster it's undefined, it's a hypothetical event. It's easy to de-prioritize it. It's not an excuse, but, as with everything in cyber security, we have to consider the human factor," he said. "Making sure that it's in their face and more tangible to them as a potential outcome for their organization will increase the likelihood that people pay attention."

Once you make it to the right side of the "boom" it becomes extremely important to minimize the amount of damage by figuring out which servers and resources have been affected and which data is encrypted. It's also crucial to make sure that backups are available so an organization can recover quickly, said Rebecca Fitzhugh, principal technologist and director of developer relations at Rubrik, especially since cyber criminals are increasingly focusing on encrypting backups.

"You can do all the right things," she explained. "You can be running up to the end point protection, you can do user education, you can do everything right, and still get attacked. It's always going to be coming back to, 'Can I recover? And how quickly can I recover?'" When a cybercriminal eliminates your last line of defense, you may have to pay the large ransom or rebuild your infrastructure from the ground up – and neither option is good.

Agencies should look for API-driven backup solutions that detect anomalies on backup data, and make sure that backup data is immutable – it is never available in a read/write format and it cannot be overwritten in any shape or form, Fitzhugh said. "Really, the concept of immutability should be back baked into your backup architecture to ensure that no security exposure can tamper with your backups. We (also) want to have some sort of mechanism for faster recovery or even automated recovery, where we can revert back to the most recent clean version, whether we use something like an instant recovery upload or file level recovery operations."

BEST PRACTICES

Here are some steps that every agency should be thinking about as ways to proactively reduce the chance of a ransomware attack:

- Creating policies around basic cyber hygiene including regular patching, creating good network segmentation, implementing air gap networks, and avoiding exposed remote desktop protocols (RDP).
- Making sure an agency has the right contract in place to ensure rapid access to backups so downtime is minimized and the mission isn't interrupted.
- Building and disseminating staffing policies and procedures so employees can be brought in quickly if there is an afterhours incident.
- Creating a playbook for ransomware so that everyone – from legal to external affairs – knows how to respond when there's an attack.
- Incorporating ransomware response into the agency's overall disaster recovery plan.
- Practicing and testing the disaster recovery plan so you know exactly what to do when you get hit and how you can quickly recover.