Ransomware in Real Life

August 2020

Imagine this: It's 2 a.m. in the hospital data center and a few servers are suddenly unavailable. The IT analyst calls CloudWave's Cloud Care Service Desk and reports the issue.

A ticket is opened, a critical incident is called and troubleshooting begins immediately. In the meantime, nurses are beginning to call the hospital help desk to report their computer is locked and they can't log in to MEDITECH. The CloudWave team quickly identifies the root cause: ransomware.

Some may not need to use their imagination to play out this scenario. Two of CloudWave's OpSus Live customers recently suffered similar situations in their on-premises data center, both due to ransomware attacks. And they are not alone. HealthIT Security recently reported on a study showing 41 U.S. healthcare organizations experienced ransomware attacks in the first half of 2020.

It's a position that no hospital wants to find itself in.

CloudWave has helped 9 hospitals recover and restore operations after a ransomware attack in the last two years. In the case of OpSus Live, Recover, and Backup customers, CloudWave's defense-in-depth security protects data in the OpSus Healthcare Cloud from the cybercriminals executing the ransomware attack. With OpSus Live hosting, CloudWave isolates the cloud production environment from the infected hospital data center after the incident. For OpSus Recover and Backup customers, CloudWave quickly recovers data in the cloud and restores access for MEDITECH to validate systems before establishing connectivity for clinicians. For our self-hosted customers, CloudWave has helped rebuild local systems, recover data where possible, and provide additional technical resources.

For our two OpSus Live customers attacked earlier this year, having their data in the cloud provided significant advantages. The OpSus team was able to cut connectivity between the infected local data center and their hosted platform, preserving their PHI and data in a secure environment. As a result, both customers avoided a breach, and neither had to pay ransom to get their hosted data back. In addition, they were able to virtually "scale" their IT team with CloudWave resources, allowing them to focus on invoking their disaster plan, support users, conduct forensics, and work with cybersecurity insurance.

"CloudWave helped our customers recover in record time.", said Alan Stavris, Supervisor of the Technical Account Managers at MEDITECH. "Efficiently migrating to the cloud from on-prem; precisely persevered the system configuration but more importantly the integrity of their patient data. We were able to swiftly validate their infrastructure and turn the system back over to the customer and OpSus team, which allowed them to expeditiously get back up and running with limited downtime."

Mark Middleton, CloudWave's Chief Quality Officer and VP of Cloud Services emphasized, "In addition to technical security controls on premises to prevent ransomware, it's imperative to have comprehensive recovery plans in the event of an attack. Part of those plans should include services and suppliers with ample human capital and knowhow to contain, isolate, and recover from an event. Recovery from major events like this can exhaust hundreds of man hours of activities and it's important be able to execute several activities in parallel, which is typically beyond what an average hospital or health system can provide. We're proud that our OpSus team is able and ready to support our customers when they need it most."

Ransomware is a threat that's not going away and continues evolve. The same HealthIT news article underscores this, reporting a recent spike in ransomware and malware variants.

We're here for you if a cyberattack happens to your data center. CloudWave can also help you prevent an attack and improve your overall security posture on premises. Combining OpSus Cloud services, which are built to protect your data in the cloud, with proactive strategies to defend your local hospital data center can offer a higher level of security against ransomware and other cyber threats. If you're interested in learning more, contact us at customersfirst@gocloudwave.com.

Source article: https://healthitsecurity.com/news/top-risks-of-1h-2020-ransomware-mobile-health-infrastructure

CloudWave