rubrik | federal

Are Federal Data Backups Safe from Ransomware? Maybe Not.

Federal agencies reported more than 35,000 cybersecurity incidents for their IT systems in the fiscal year ending September 2017, with thousands of these cases involving phishing emails carrying advanced malware or ransomware, according to OMB's 2018 annual FISMA report to Congress.[1]

Staying ahead of cyber adversaries is a top priority for Federal leaders, and President Trump's Cybersecurity Executive Order holds agency leaders accountable for cyber risk management. The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program is moving forward into its third phase, improving agencies' awareness of their environment, their vulnerabilities, and implementing consistent best practices.[2] And, the next FITARA (Federal Information Technology Acquisition Reform Act) Scorecard grading set for May 2019 is likely to incorporate evaluations of cyber hygiene, bringing additional transparency to security efforts across government.

But while there's a lot going on to boost Federal network security, there is still much to be done.

Even as the volume and sophistication of cyber attacks continue to grow, the Government Accountability Office reported in December 2018 that 17 out of 23 civilian Chief Financial Officers Act (CFO Act) agencies have not yet fully implemented effective security programs, leaving them vulnerable to future attacks.[3] Poor data management exposes organizations to the threat of compromised information and the potential loss of backup data, thus eliminating recovery capabilities.

With the evolution of ransomware and other attack methods, just how vulnerable are agencies today and what preventative measures can they take to mitigate risk?

Securing Complex Environments

Most Federal agencies manage legacy systems with complex data backup agents. These backup systems, designed for on-premise data centers, are largely incompatible with multi-cloud and hybrid cloud environments—making it difficult to identify and respond to threats. In response, many organizations are tiering data and applications, using different backup systems and methodologies to protect each depending on where they reside. Unfortunately, this creates more complexity and reduces the ability to respond quickly to breaches.

Adversaries Are Getting Smarter

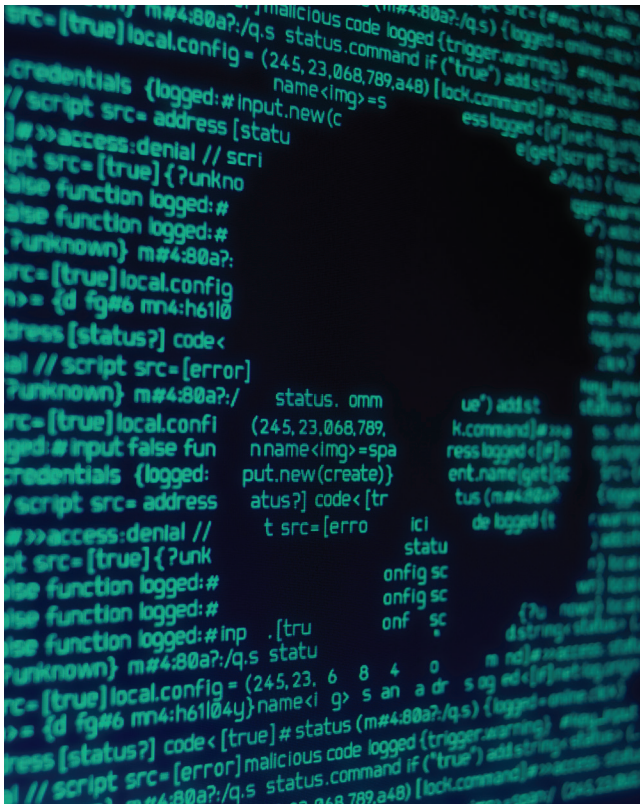
While cybersecurity has taken a front seat for both Federal and enterprise customers, ransomware attacks are still growing more than 350% annually.[4] And they are getting more dangerous. Ransomware attacks today can also target backup data. Attacks sit dormant, gathering critical information, such as system logins, before compromising the entire system and backup in one attack. Because these new methods are unexpected, responding and recovering information can take months or years, if ever achieved. In many cases, these attacks make backup data completely unrecoverable. Administrators and agencies are far more likely to pay "ransom" money to attackers when their recovery operations are stunted. Federal agencies need to enhance their data protection to include measures that ensure backup data is never exposed in the first place.

1 https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReport-Congress.pdf
2 https://www.meritalk.com/articles/cdm-program-to-issue-cyber-hygiene-score-in-fy20/
3 https://www.gao.gov/assets/700/696105.pdf

4 Cisco 2017 Annual Cybersecurity Report

Holistic Response and Recovery: Less is More

While attacks are becoming more complex, the answer is not necessarily a solution that matches that complexity. Holistic response strategies that consider both data protection and recovery, and spanning on-premise and hybrid cloud environments, are critical. Additional layers of security, including immutability measures, can help protect data copies from ransomware attacks. In the case of an attack, these measures provide instant recovery and shorten what could be a lengthy reparation process. Administrators should prioritize data management and application recovery, as these components can be easily reproduced and restored without a tedious process.



Rubrik: Immutability to Defend Against Ransomware

Rubrik, the market leader in Cloud Data Management, provides a single software platform to automate, govern, and secure applications and data on-premises and in the cloud. Rubrik's Cloud Data Management platform enables agencies to quickly recover from ransomware attacks with just a few clicks.

Rubrik captures all data in an immutable format, preventing ransomware from ever accessing and encrypting the backup files. Combined with incremental-forever backups and point-in-time recovery, these factors can save agencies hundreds of hours while minimizing operational disruptions and data loss.

The bad actors may be getting smarter and the threats ever more dangerous, but a more sophisticated, highly resilient data management and backup strategy can prevent an attack from becoming a disaster. As Federal leaders look to improve cyber hygiene, they must consider their cloud strategies, backup requirements, and overall objectives to ensure cyber attacks are stopped in their tracks.

Learn more: https://www.rubrik.com/solutions/ransomware-recovery/