White Paper

For a Successful Digital Transformation, Government Must Leverage Third-Party Backup

Today, more state and local governments are adopting cloud-based productivity tools such as Microsoft Office 365. Relying on Microsoft's native backup capabilities isn't enough to protect organizations from data loss. Instead, a third-party backup solution is critical to IT success.

A surge in remote work and IT modernization efforts have pushed state and local governments toward cloud-based productivity tools, such as Microsoft Office 365, for collaboration. But relying on this solution to manage data and compliance isn't enough; a third-party tool is crucial to ensure an organization's data is backed up — especially in a worst-case scenario such as a ransomware attack.

In 2019, at least 966 government agencies, educational establishments and health care providers fell victim to ransomware attacks. Of those, 113 were state, municipal governments and agencies, according to a report by global cybersecurity company Emsisoft. This year alone, 60 government entities — including cities, transportation agencies and police departments — were impacted by ransomware attacks.

As state and local governments continue to be in the hackers' crosshairs, ransomware attacks are resulting in the biggest source of data loss from breaches, according to Jeff Reichard, senior director of enterprise strategy at Veeam, a cloud data management provider to federal, state and local governments.

"The financial loss and the losses of service are tremendous," he said.

As more organizations move to Microsoft Office 365 for tools such as Teams, Exchange and OneDrive, a growing number of ransomware attacks can pose as Microsoft Office documents or as links in emails.

"The uptick in Office 365 is huge for obvious, good reasons, but that's an uptick in the exact vector that most ransomware attacks, which are the most damaging kind of attacks, use," Reichard said.

Relying on Microsoft's native backup capabilities isn't enough to protect organizations from data loss. To ensure an organization can fully recover data that hasn't been compromised by malware after a ransomware attack, data may need to be restored from months prior. Microsoft's native backup capabilities can't do that by default, so the company recommends a third-party backup solution.

966

government agencies, educational establishments and health care providers fell victim to ransomware attacks in 2019.

Source: The State of Ransomware in the US: Report and Statistics 2019, Emsisoft, https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

© 2020 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Where Data Owners Fall Short

Microsoft's shared responsibility model, though readily available and common with cloud providers, is sometimes not fully realized. The model varies depending on cloud use, but ultimately, the customer retains responsibility for information and data.

This means the data owner is on the hook for meeting regulatory data requirements, especially if those requirements extend past Microsoft's default data retention of 30 days for deleted items. That can be changed, but it's not often done. And items can be set to auto-archiving, but once deleted in archives, they are transported to the recycle bin and permanently deleted after 90 days.

If local and state government agencies must answer regulatory compliance requests for privacy violations, for instance, they can be subjected to litigation and discovery. But claiming the data was automatically deleted after 30 days won't cut it.

"You need to be able to produce the documents in a responsive way," Reichard said. "If the public sector wants to be really responsive to potential litigation and to be compliant with different kinds of regulation at all levels, they need a backup tool that will let them get all their data back for a given point in time."

Veeam's recent "2020 Data Protection Trends," report, which surveyed over 1,500 senior business and IT decision-makers across the globe, found 73% of respondents didn't meet their own service-level agreements for file recovery capabilities. More than 80% of respondents experienced data loss in Office 365, including simple user errors all the way up to major data security threats.

"It is truly terrifying that over two-thirds of the folks that we surveyed are relying on the native backup capabilities or the native data protection capabilities in Office 365," Reichard said.

That's where third-party backup comes in. A solution such as *Veeam Backup for Microsoft Office 365* could help, as it complements the built-in data management features in Office 365 to provide regulatory compliance and deliver full data backup and recovery capabilities. It also enables agencies to quickly comply with all legal discovery requests.

> "It is truly terrifying that over two-thirds of the folks that we surveyed are relying on the native backup capabilities or the native data protection capabilities in Office 365."
>
> **— Jeff Reichard,**
> **Senior Director, Enterprise Strategy, Veeam**

© 2020 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

The Trinity of Data Protection

When looking for backup capabilities, Reichard said customers should consider three things: data recovery to a point in time, data portability and granular restore capabilities — all of which are included in Veeam Backup *for Microsoft Office 365*.

The solution can recover data from a specific point in time, rather than relying on a recycle bin that retrieves individual items on an ad-hoc basis. Data portability allows users to back up data into cross-cloud or on-premise platforms, extending from the physical to the virtual environment. This way, customers aren't locked into a single cloud service provider.

Rather than just restoring item by item or entire environments, granular restore capabilities allow users to restore items as different (or more up-to-date) file formats. Veeam also provides scalability to large environments as customers with over 20,000 mailboxes are protecting their data with the solution.

But ransomware attacks aren't the only instances where data can be erased or lost.

In Office 365, technical storage blips can also occur, where data is permanently lost because of issues with hardware and software configurations. Users can also lose data access to a domain name system issue.

"It's not just actually preventing data loss; it's also preventing loss of access to data," Reichard said. "Even though the Office 365 service is fantastic, resilient and being migrated to for a lot of good reasons, that doesn't mean it's perfect. We need to plan around different contingencies."

Plus, Veeam's backup solution can provide a local copy of data needed for compliance or regulatory reasons, even amid cyberattacks or technical errors.

> "It's not just actually preventing data loss; it's also preventing loss of access to data."
>
> **— Jeff Reichard, Senior Director, Enterprise Strategy, Veeam**

The Total Package

The sentiment in the public sector is clear: If considering transformation initiatives and cloud migrations, the sooner, the better. With increasing virtual work environments, collaboration and cloud services are key.

But that doesn't mean forgoing data protection.

"If folks are moving to Office 365, they need to follow Microsoft best practices and use a third-party backup tool," Reichard said.

And when choosing a data protection partner, Reichard recommends looking carefully at long-term sustainability and vendor viability. Because organizations don't have to compromise for data protection and recovery, especially as a means of preparing for and fortifying against ransomware attacks and other potential data-loss events.

Learn more about how you can take control of your data with Veeam Backup *for Microsoft Office 365*.

© 2020 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.